SIEMENS

SIMATIC NET

Industrial Ethernet Wireless LAN
RLM Manager
CP 1515 Manager

Handbuch

C79000-G8900-C171-01
Ausgabe 11/2001

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft und notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten. Für Verbesserungsvorschläge sind wir dankbar.

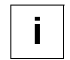
Siemens AG 2001
Bereich Automatisierungs- und Antriebstechnik
Geschäftsgebiet Industrie-Automatisierungssysteme
Postfach 48 48, D-90327 Nürnberg

C79000-G8900-C171-01

Siemens Aktiengesellschaft

Klassifizierung sicherheitsrelevanter Hinweise

Dieses Handbuch enthält Hinweise, die Sie zur Gewährleistung Ihrer eigenen Sicherheit sowie zum Schutz des Produktes und der angeschlossenen Geräte unbedingt beachten sollten. Diese Hinweise sind je nach Grad der Gefährdung wie nachfolgend beschrieben gekennzeichnet:



HINWEIS:

Hinweise enthalten wichtige Informationen zum Produkt selbst oder zu dessen Einsatz. Das "i" kennzeichnet die Teile der Dokumentation, die sehr wichtig und für den Benutzer besonders nützlich sind.



WARNUNG:
Weist auf Gefahren für Leib und Leben hin.



ACHTUNG:
Achtung-Hinweise mit dem Warndreieck weisen auf Gefahren hin, die zu weniger schweren Verletzungen führen können.

ACHTUNG:

Achtung-Hinweise ohne Warndreieck signalisieren Gefahren, die zur Beschädigung oder Zerstörung der Hard- bzw. Software führen können.

Marken

SIMATIC®, SIMATIC NET® und SIMATIC NET Networking for Industry® sind eingetragene Marken der Siemens AG.

Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen können.

Sicherheitstechnische Hinweise zu Ihrem Produkt

Bevor Sie das hier beschriebene Produkt einsetzen, beachten Sie bitte unbedingt die nachfolgenden sicherheitstechnischen Hinweise.

Qualifiziertes Personal

Inbetriebsetzung und Betrieb eines Gerätes dürfen nur von qualifiziertem Personal vorgenommen werden. Qualifiziertes Personal im Sinne der sicherheitstechnischen Hinweise dieses Handbuchs sind Personen, die die Berechtigung haben, Geräte, Systeme und Stromkreise gemäß den Standards der Sicherheitstechnik in Betrieb zu nehmen, zu erden und zu kennzeichnen.

Bestimmungsgemäßer Gebrauch von Hardware–Produkten

Beachten Sie bitte folgendes zum bestimmungsgemäßen Gebrauch von Hardware–Produkten:

Vorsicht

Das Gerät darf nur für die im Katalog und in der technischen Beschreibung vorgesehenen Einsatzfälle und nur in Verbindung mit von Siemens empfohlenen bzw. zugelassenen Fremdgeräten und -komponenten verwendet werden.

Der einwandfreie und sichere Betrieb des Produktes setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung und Montage sowie sorgfältige Bedienung und Instandhaltung voraus.

Bevor Sie mitgelieferte Beispielprogramme oder selbst erstellte Programme anwenden, stellen Sie sicher, dass in laufenden Anlagen keine Schäden an Personen oder Maschinen entstehen können.

EG–Hinweis: Die Inbetriebnahme ist so lange untersagt, bis festgestellt wurde, dass die Maschine, in die diese Komponente eingebaut werden soll, den Bestimmungen der Richtlinie 89/392/EWG entspricht.

Bestimmungsgemäßer Gebrauch von Software–Produkten

Beachten Sie folgendes zum bestimmungsgemäßen Gebrauch von Software–Produkten:

Vorsicht

Die Software darf nur für die im Katalog und in der technischen Beschreibung vorgesehenen Einsatzfälle und nur in Verbindung mit von Siemens empfohlenen bzw. zugelassenen Software-Produkten, Fremdgeräten und -komponenten verwendet werden.

Bevor Sie mitgelieferte Beispielprogramme oder selbst erstellte Programme anwenden, stellen Sie sicher, dass in laufenden Anlagen keine Schäden an Personen oder Maschinen entstehen können.

Vor der Inbetriebnahme

Beachten Sie vor der Inbetriebnahme folgende Warnung:

Vorsicht

Vor der Inbetriebnahme sind die Hinweise in der entsprechenden aktuellen Dokumentation zu beachten. Diese finden Sie auf der CD "SIMATIC NET Wireless LAN, System Software, Manuals" sowie im Internet unter **www.siemens.com/mobic**.

Vorwort

Zweck des Handbuches

Dieses Handbuch soll Sie bei der Konfiguration, Inbetriebnahme und Fehlerbeseitigung von Netzen, die den Industrial Ethernet Wireless LAN Manager und CP 1515 Manager umfassen, unterstützen.

Weitere Dokumentation

Die Handbücher

- "SIMATIC NET Industrial Ethernet Twisted Pair and Fiber Optic Networks"
- "SIMATIC NET Industrial Ethernet Wireless LAN, Basics"
- "SIMATIC NET Industrial Ethernet Wireless LAN, RLM"
- "SIMATIC NET Industrial Ethernet Wireless LAN, CP 1515"

enthalten Informationen zu weiteren SIMATIC NET-Produkten, die Sie in Kombination mit dem RLM Manager und CP Manager in einem Industrial Ethernet-Netz einsetzen können.

Alle Handbücher befinden sich auf der im Lieferumfang Ihres Produktes enthaltenen CD-ROM "SIMATIC Net Wireless LAN, Systemsoftware and Manuals".

Zu diesem Handbuch

Damit Sie die benötigten Informationen schnell finden, ist dieses Handbuch wie folgt aufgebaut:

- Vor den eigentlichen Bedienungsanweisungen finden Sie ein vollständiges Inhaltsverzeichnis.
- Die Kapitel haben Kopfzeilen am linken Rand mit einer Inhaltsübersicht der Absätze des jeweiligen Abschnitts.
- Hinten in dem Handbuch finden Sie einen Index, mit dessen Hilfe Sie schnell zu den jeweils gewünschten Themen gelangen.
- Das Handbuch "Industrial Ethernet Wireless LAN, Basics" enthält ein Glossar, das die wichtigsten in diesen Anweisungen benutzten Fachbegriffe definiert.

Zielgruppe

Dieses Handbuch richtet sich an Personen, die für die Konfiguration und Inbetriebnahme von Netzen, einschließlich RLM, CP 1515, RLM Manager und CP Manager, sowie für die Fehlerbeseitigung in derartigen Netzen zuständig sind.

Anforderungen an das Bedienungspersonal

Nur qualifiziertem Personal sollte die Installation und Benutzung dieses Geräts gestattet werden.
Qualifiziertes Personal gemäß den Bedienungsanweisungen oder Warnhinweisen ist definiert als Personen, die mit der Installation, Montage, Inbetriebnahme und Bedienung dieses Produktes vertraut sind und die für Ihre Tätigkeiten erforderlichen Qualifikationen besitzen, z.B.:

- Training oder Befugnis für Anschluss, Erdung oder Kennzeichnung von Leitungen und Geräten oder Systemen gemäß den aktuellen Standards der Sicherheitstechnologie;
- Training oder Befugnis für die Wartung und den Einsatz geeigneter Sicherheitssysteme gemäß den aktuellen Standards der Sicherheitstechnologie.

Normen und Zulassungen

SIMATIC NET Wireless LAN Produkte erfüllen die Anforderungen für die CE-Kennzeichnung. Genauere Einzelheiten zu Zulassungen und Normen können dem Handbuch "Industrial Ethernet Wireless LAN, Grundlagen" entnommen werden.

Inhaltsverzeichnis

A Startkonfiguration

B Problembehandlung

C Erzwungener Neustart

D Aktualisieren der RLM-Software

E Weitere Unterstützung

1 Einführung

1.1 Allgemeines zu Siemens SIMATIC NET IWL

Die Produktfamilie Siemens SIMATIC NET IWL (IWL) umfasst ein umfangreiches Paket von Netzkomponenten, mit deren Hilfe Sie die verschiedensten Netzkonfigurationen erstellen können - angefangen von kleinen unabhängigen IWL-Netzen bis hin zu großen, durchgängig drahtlosen Infrastrukturen. Zur Produktfamilie Siemens SIMATIC NET IWL gehört ein Radio Link Modul (RLM), über das drahtlose Stationen in die bestehende leitungsgebundene Ethernet LAN-Infrastruktur eingebunden werden können.

Die IWL-Netzschnittstelle unterscheidet sich nur geringfügig von der Schnittstelle eines leitungsgebundenen LAN. Für das Betriebssystem ist dieser Unterschied überhaupt nicht wahrnehmbar.

Wie Kommunikationsprozessoren (CP) für leitungsgebunden Netze werden Wireless LAN CPs wie der CP 1515 mit einem dedizierten SIMATIC NET IWL-Treiber installiert, wobei für den Anschluss ans Netz kein Kabel benötigt wird. Bei der Verwendung des Wireless LAN CPs CP 1515 können Workstations umgezogen werden, ohne dass hierfür Änderungen an der Verkabelung im Netz oder den Anschlüssen an Patchfeldern oder Hubs notwendig sind.

1.2 Allgemeines zu den SIMATIC NET IWL-Tools

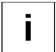
Die Software-Suite SIMATIC NET IWL besteht aus einer Reihe von Management-Tools, die folgende Maßnahmen erlauben:

- Anzeigen und Ändern der Konfiguration von (entfernten) Netzkomponenten
- Konfigurieren von Netzkomponenten wie etwa Radio Link-Modulen
- Analysieren der Netz-Performance und ggf. Erkennung und Behebung von Netzfehlern
- Management und Optimierung der Netz-Performance

Die Software-Suite SIMATIC NET IWL umfasst folgende Tools:

- CP 1515 Manager
- RLM Manager

Die Installation der SIMATIC NET IWL-Tools ist auf Stationen mit den Betriebssystemen Microsoft Windows 98 , ME, NT V4.0 oder 2000 möglich.



HINWEIS:

Die Produkte der Familie SIMATIC NET IWL sind für den Betrieb mit sämtlichen Drahtlos-LAN-Produkten ausgelegt, die mit der Direktsequenz-Funktechnologie gemäß dem Standard IEEE 802.11 arbeiten.

Die SIMATIC NET IWL-Hardware kann mit Drahtlos-LAN-Produkten anderer Hersteller, die der IEEE 802.11 entsprechen, kommunizieren.

Dagegen ist die Software-Suite SIMATIC NET IWL unter Umständen nicht immer zusammen mit Fremdhersteller-Produkten einsetzbar, und zwar aus folgenden Gründen:

- Im Standard IEEE 802.11 für drahtlose LANs sind keine Normen für Diagnose- und Management-Tools festgelegt, so dass die einzelnen Hersteller möglicherweise jeweils eigene Tools für die Konfiguration und das Management von Wireless-LANs gemäß IEEE 802.11 konzipiert haben.
- Die Software-Suite SIMATIC NET IWL bietet eine umfangreiche Palette von Tools zur Überwachung und Auswertung verschiedenster Diagnosezähler.

  Für einige dieser Tools sind Zusatzfunktionen in der Hardware erforderlich, die von den Produkten der Familie SIMATIC NET IWL standardmäßig unterstützt werden, von den Produkten anderer Hersteller unter Umständen jedoch nicht.

Wenn Abfragen der Verbindungsqualität oder Konfigurationsparameter von Fremdhersteller-Produkten mit der Software-Suite SIMATIC NET IWL nicht möglich sein sollten, schlagen Sie bitte in der Dokumentation zum Fremdhersteller-Produkt nach.

1.2.1 CP 1515 Manager

Beim CP 1515 Manager handelt es sich um ein Diagnose-Tool zur Überwachung der Funkverbindung zwischen einer IWL-Station und dem zugehörgen Access Point RLM bzw. zur Überwachung der Verbindung zwischen zwei drahtlosen Stationen in einem unabhängigen Netz.

Daneben lässt sich das Tool als Site Monitor zur Anzeige der Reichweite des Access Point RLM in einem bestimmten Bereich einsetzen.

1.2.2 RLM Manager

Der RLM Manager ist in erster Linie ein Tool für LAN-Administratoren bzw. Systembetreuer. Mit Hilfe des Programms RLM Manager können Sie Radio Link Modules (RLMs) konfigurieren und die Performance des Wireless-LAN überwachen. Das Programm lässt sich auf jeder beliebigen Station (leitungsgebunden oder drahtlos) im Netz ausführen.



ACHTUNG:
Das setzen von Parametern setzt den RLM zurück, es erfolgt ein Neuanlauf (reboot) und die Kommunikation zum und über den Accesspoint RLM ist für mindestens 15 Sekunden unterbrochen.

1.3 Allgemeines zu SIMATIC NET IWL RLM

Das Radio Link Module RLM arbeitet als transparente Bridge zwischen bis zu zwei Wireless LANs und einem drahtgebundenen LAN. Geräte mit dieser Funktion werden auch als "Access Point" bezeichnet. Das RLM ist mit zwei Steckplätzen A und B für die Aufnahme von PCMCIA-Karten ausgrüstet. Die Wireless LAN Schnittstellen A und B entsprechen den Steckplätzen A und B, die mit IWL CPs vom Typ CP 1515 bestückbar sind.

Die Access Point RLM werden jeweils über eine der folgenden MAC-Adressen identifiziert:

- Die universelle MAC-Adresse der im Access Point RLM benutzten IWL CPs CP 1515 oder
- Die universelle MAC-Adresse der Ethernet-Schnittstelle.

Weitere Angaben zu den Produkten der Familie SIMATIC NET IWL entnehmen Sie bitte der mitgelieferten Dokumentation, oder besuchen Sie unsere Website unter **http://www.siemens.com/mobic**.

1.4 Zum vorliegenden Benutzerhandbuch

Das vorliegende Handbuch beschreibt, wie Sie mit Hilfe der SIMATIC NET IWL-Tools drahtlose LANs konfigurieren und überwachen können, die mit Produkten der Familie SIMATIC NET IWL eingerichtet wurden.

Das Handbuch enthält folgende Punkte:

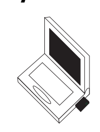
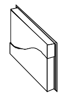
- 1 "Einführung" enthält Beschreibungen zu den SIMATIC NET IWL-Tools und Hinweise zu zusätzlichen Informationsquellen.
- Das Kapitel 2 "Drahtlos-Konfigurationen" beschreibt Netzszenarien, auf die im vorliegenden Dokument des Öfteren zurückgegriffen werden wird.
- Unter 3 "Einrichten der LAN-Administratorstation" ist beschrieben, wie Sie eine Station als Management-Terminal für das SIMATIC NET IWL-Netz einrichten können und die entsprechende Software installieren.
- Im Kapitel 4 "Einfache Netzkonfigurationen" wird anhand dreier Beispiele (von einfach bis anspruchsvoll) die konkrete Konfigurierung des Netzs erläutert.
- Unter 5 "Überwachen des SIMATIC NET IWL-Netzes" sind Maßnahmen zur Überwachung und Diagnose der Verbindungsqualität beschrieben.
- Kapitel 6 "Optimierung der Leistungsfähigkeit" enthält einige Überlegungen, die Ihnen das Verständnis der komplexen Faktoren erleichtern sollen, von denen die Performance eines Drahtlos-Netzes abhängt.
- Unter 7 "Sicherheit" werden Maßnahmen zur Erhöhung der Sicherheit und zur Vermeidung unbefugter Zugriffe auf das SIMATIC NET IWL-Netz erläutert.

Das vorliegende Dokument beschreibt hierbei nicht sämtliche mögliche Funktionen, die von der Software-Suite SIMATIC NET IWL unterstützt werden, sondern versteht sich als allgemeine Richtlinie, die Ihnen bei der Entscheidung helfen soll, welches Tool für eine bestimmte Aufgabe am geeignetsten ist.

Zusätzliche Angaben zu bestimmten Masken der Bedienoberfläche oder zu Programmfunktionen entnehmen Sie bitte der Online-Dokumentation.

1.4.1 Im vorliegenden Dokument verwendete Symbole

Im vorliegenden Dokument werden die verschiedenen Netzkomponenten durchgängig mit folgenden Symbolen dargestellt:

Symbol	Beschreibung
	**Drahtloser Computer** mit: • PC-Karte (CP 1515)
	**Access Point** • Radio Link-Modul (RLM)

1.4.2 Online-Hilfe

Angaben zu bestimmten Masken der Bedienoberfläche oder Funktionen der Tools RLM Manager bzw. CP 1515 Manager sind in der Online-Hilfe der jeweiligen Programme enthalten.

- Um die Kontexthilfe zu einem bestimmten Fenster eines der SIMATIC NET IWL-Programme aufzurufen, klicken Sie auf die Schaltfläche **Help** oder drücken Sie die Funktionstaste F1 .
- Durch Anklicken der Registerkarte **Contents** in der Online-Hilfe rufen Sie eine Übersicht der vorhandenen Informationen auf; unter der Registerkarte **Index** erscheint eine alphabetische Auflistung der einzelnen Hilfe-Themen.

Technische Produktangaben sind in den jeweiligen Benutzerhandbüchern zu den SIMATIC NET IWL-Produkten aufgeführt.

1.4.3 Zusätzliche Dateien auf der CD-ROM

Die zusammen mit den SIMATIC NET IWL-Produkten ausgelieferte CD-ROM enthält eine Datei mit dem Namen "liesmich.rtf". Diese enthält Angaben zur jeweiligen Software-Version und/oder zu den Treibern auf der CD-ROM.

Es wird empfohlen, vor Installation der SIMATIC NET IWL-Produkte diese Datei durchzulesen, die diese möglicherweise zusätzliche Informationen enthält, die zum Zeitpunkt der Fertigstellung dieses Handbuchs noch nicht vorlagen. Daneben liegt die Datei "liesmich.rtf" auch auf der SiemensWebsite
http://www.siemens.com/mobic zum Ansehen und Downloaden bereit.

1.4.4 Zusätzliche Informationsquellen

Informationen zu Updates und aktuelle Neuigkeiten zu Siemens finden Sie unter **http://www.siemens.com/mobic**.

Angaben zum Technischen Support finden Sie am Ende des vorliegenden Dokuments.

2 Drahtlos-Konfigurationen

2.1 Einführung

Das vorliegende Dokument beschreibt mehrere Netzszenarien, die Sie beim Einrichten eines Drahtlos-Systems als Muster heranziehen können. Drahtlos-Systeme findet man normalerweise in Netzumgebungen in geschlossenen Räumen vor, wo sie eine Anschlussmöglichkeit für Geräte bieten, die innerhalb des Netzes häufiger den Standort wechseln.

Unter einem Drahtlos-System versteht man dabei ein drahtloses Netz, über das drahtlose (mobile) Geräte versorgt werden. Die drahtlosen Geräte können innerhalb des Netzes den Standort beliebig wechseln, wobei sich Einschränkungen durch die Größe und Reichweite des Geräts ergeben können.

Je nach Größe und Anforderungen des LAN lassen sich Drahtlos-Systeme einem der folgenden Konfigurationstypen zuordnen:

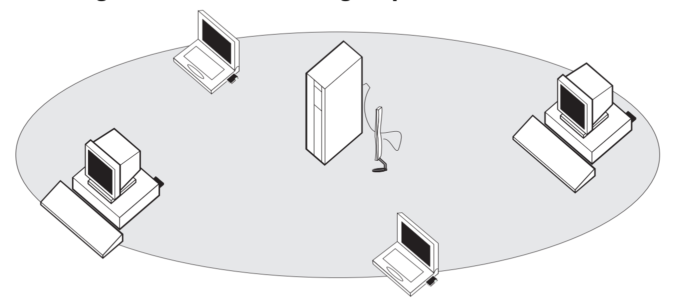
- Unabhängiges Netz
- Einfache Infrastruktur
  1. Standalone-Konfiguration
  2. Funkzugang zu Ethernet-Netzen
- Komplexe Infrastrukturen
  1. Mehrkanal-Konfiguration

2.2 Peer-to-Peer-Workgroup

Eine Peer-to-Peer-Workgroup (siehe Darstellung in Abbildung 1) ist eine Gruppe von drahtlosen Geräten, bei denen Daten nicht über das Radio Link Module (RLM) gebridged werden. Innerhalb eines Peer-to-Peer-Netzes werden sämtliche Rechner als "Peer-to-Peer" konfiguriert.

Die einfachste Variante eines unabhängigen Netz ist ein Netz ohne Server, bei dem die einzelnen Stationen im Peer-to-Peer-Modus miteinander kommunizieren und z.B. über ein Microsoft-Netz auf eine gemeinsame Festplatte oder einen Drucker zugreifen.

Abbildung 1 Peer-to-Peer-Workgroup



Peer-to-Peer-Konfigurationen finden normalerweise in kleinen Netzen Verwendung, wo folgende Voraussetzungen gegeben sind:

- Sämtliche IWL-Stationen führen Workgroup-Funktionen aus und greifen beispielsweise über das Microsoft-Netz auf eine gemeinsame Festplatte und auf Drucker zu.

- Sämtliche Stationen befinden sich innerhalb der Reichweite eines Drahtlos-Servers.

Peer-to-Peer-Konfigurationen stellen eine pratische Lösung zum Einrichten eines Drahtlos-Netzes für Messen, Kundenbesuche oder andere Außen-Einsätze dar.

2.3 Einfache Infrastrukturen

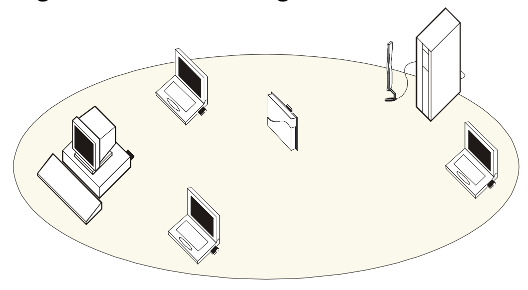
2.3.1 Standalone-Konfiguration

Bei einer Standalone-Konfiguration (Abbildung 2) fungiert das Radio Link Module (RLM) als Relais-RLM, das innerhalb derselben Funkzelle Daten von einem Computer zum nächsten weiterreicht.

Hierbei handelt es sich um die schnellste und einfachste Methode zum Einrichten einer kleinen Drahtlos-LAN-Infrastruktur. Diese Konfiguration eignet sich besonders für zeitlich befristete Installationen in Umgebungen, wo die Installation einer leitungsgebundenen Infrastruktur nicht möglich ist (z.B. auf Messen).

Ein Server wird bei einer Standalone Drahtlos-Konfiguration nicht benötigt; entsprechend ausgestattete Geräte können wie in Abbildung 2 Standalone-Konfiguration dargestellt im Peer-to-Peer-Modus miteinander kommunizieren.

Abbildung 2 Standalone-Konfiguration



Das Drahtlos-Netz wird dabei über einen eindeutigen Netznamen identifiziert. Sämtliche Geräte, über die eine Verbindung zum Netz hergestellt werden soll, müssen mit dem selben Netznamen konfiguriert werden.

Mobile drahtlose Stationen bleiben mit dem Netz in Verbindung, solange sie sich innerhalb der Reichweite des Access Point RLM im jeweiligen SIMATIC NET IWL-Netz befinden.

2.3.2 Funkzugang zu Ethernet-Netzen

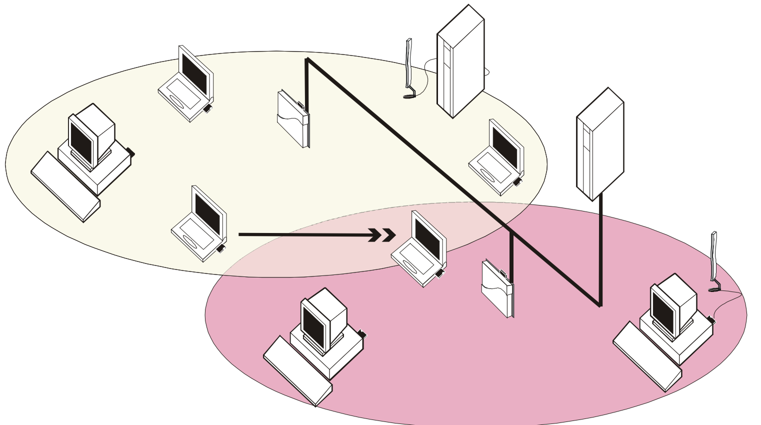
Mit der Einbindung eines Access Point RLM in ein Ethernet-Netz (siehe Darstellung in Abbildung 3 Konfiguration für Funkzugang zu einem Ethernet-Netz) ergeben sich folgende Möglichkeiten:

- Einrichten einer Drahtlos-Umgebung für tragbare Computer

Einfache Infrastrukturen

- Anschluss mehrerer drahtloser Stationen in einer bestehenden Ethernet-Infrastruktur und damit Schaffung eines größeren Funkabdeckungsbereichs.

Abbildung 3 Konfiguration für Funkzugang zu einem Ethernet-Netz



Sämtliche IWL-Stationen innerhalb des Funkabdeckungsbereichs, über die eine Verbindung zum Netz hergestellt werden soll, müssen mit dem selben Netznamen wie die Access Points (RLMs) konfiguriert sein.

Falls erforderlich, schalten drahtlose Stationen beim Roaming automatisch zwischen den RLMs um und erhalten so die Funkverbindung zum Netz aufrecht.

2.4 Komplexe Infrastrukturen

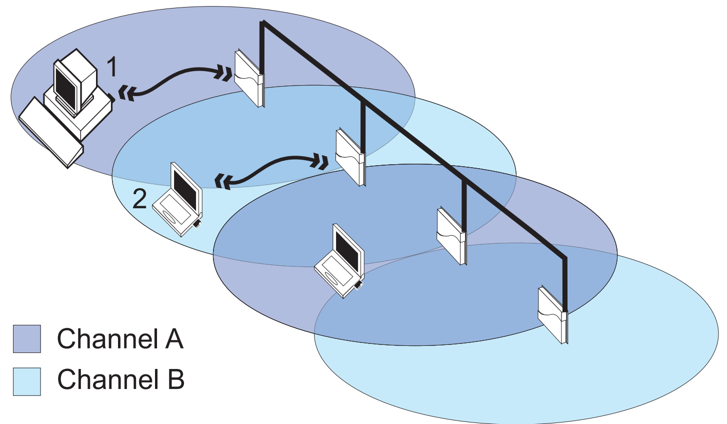
2.4.1 Mehrkanal-Konfiguration

Beim Roaming zwischen Access Points (RLMs), für die unterschiedliche Funkkanäle eingerichtet wurden, können die Stationen dynamisch zwischen verschiedenen Arbeitsfrequenz-Kanälen umschalten.

Durch die Verwendung verschiedener Kanäle und die Vergabe unterschiedlicher Frequenzkanäle für benachbarte Access Points (RLMs) lässt sich die Performance des Drahtlos-Netzes verbessern. Mehrfrequenz-Konfigurationen können sich in Umgebungen als nützlich erweisen, für die folgendes zutrifft:

- Es besteht eine hohe Konzentration von IWL-Stationen.
- Durch das CA (Collision Avoidance)-Protokoll kommt es bei den Stationen zu einer Performance-Verschlechterung hinsichtlich der Antwortzeiten im Netz (weitere Hinweise siehe "RTS/CTS-Medienreservierung (Seite 145)").

Abbildung 4 Zweikanal-Konfiguration



- Durch Einrichten unterschiedlicher Frequenzen für benachbarte Access Points (RLMs) schaffen Sie für jede Funkzelle jeweils ein eigenes Medium. Da die einzelnen Stationen mit verschiedenen Kanälen arbeiten, können sie sich untereinander nicht mehr "hören" und müssen somit nicht mehr zeitversetzt kommunizieren.
- Handelte es sich bei der in Abbildung 4 Zweikanal-Konfiguration dargestellten Konfiguration um ein Einkanal-System, müssten sich Station 1 und Station 2 dasselbe Medium teilen. Der Datenaustausch

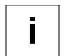
zwischen Station 1 und dem Access Point RLM müsste entsprechend verzögert werden, wenn Station 2 bereits mit dem Access Point RLM in der benachbarten Zelle kommuniziert.

Wie bei Roaming-Umgebungen grundsätzlich üblich, müssen bei einer Mehrkanal-Konfiguration sämtliche Access Points (RLMs) mit dem selben Netznamen konfiguriert sein.

Der Kanalabstand zwischen benachbarten Zellen beträgt idealerweise 25 MHz (5 Kanäle). Je nach den im jeweiligen Land verfügbaren CP 1515 kann im Drahtlos-Netz mit bis zu drei verschiedenen Kanälen gearbeitet werden (siehe den Punkt Tabelle 2 Empfohlene Unterkanal-Konfigurationen zu den empfohlenen Kanalkonfigurationen).

Beim Einsatz zweier Kanäle mit dem höchstmöglichen Kanalabstand wird der Nebensprech-Effekt zwischen den Kanälen stark verringert und somit eine spürbare Performance-Verbesserung gegenüber Netzen mit einem geringen Kanalabstand erzielt.

Hinweise zum Einrichten von Netzen mit mehreren Kanälen entnehmen Sie bitte dem Abschnitt "Verwaltung der Frequenzkanäle (Seite 153)".



HINWEIS:

Um RLMs und CP 1515 managen zu können, müssen Sie diese mit IP-Adressen versorgen (siehe Abschnitt Über IP-Adressen und Subnetze (Seite 257)).

3 Einrichten der LAN-Administratorstation

3.1 Einführung

SIMATIC NET IWL-Netze werden von der LAN-Administratorstation verwaltet. Im vorliegenden Kapitel werden Kriterien behandelt, die bei der Einrichtung eines oder mehrerer LAN-Administratorplätze zur Netzverwaltung zu beachten sind.

Bei der LAN-Administratorstation handelt es sich um einen Computer, über den der LAN-Administrator das Netz konfigurieren, verwalten und überwachen kann. Je nach Erfordernis können beliebig viele LAN-Administratorplätze eingerichtet werden.

Die Konfigurierung und Überwachung des Netzes an der LAN-Administratorstation erfolgt mit Hilfe der in der Software-Suite SIMATIC NET IWL enthaltenen Tools. Zur Software-Suite SIMATIC NET IWL gehören dabei die folgenden Programme:

- CP 1515 Manager
- RLM Manager

Im vorliegenden Kapitel ist die Einrichtung der LAN-Administratorstation in den folgenden Netzkonfigurationen beschrieben:

- **Peer-to-Peer-Workgroup** - Sämtliche Stationen im Netz kommunizieren ohne Umwege direkt miteinander. Es sind keine Access Points (RLMs) zum Bridgen der Daten erforderlich.
- **Infrastruktur-Netz** - Sämtliche Stationen kommunizieren untereinander und mit dem Ethernet Backbone über Access Point RLM-Schnittstellen.

Nähere Angaben zu den zur SIMATIC NET IWL-Software gehörenden Tools entnehmen Sie bitte dem Abschnitt "Allgemeines zu den SIMATIC NET IWL-Tools" (Seite 17).

3.2 Einrichten einer LAN-Administratorstation

3.2.1 Mindestanforderungen

Die LAN-Administratorstation kann auf jedem beliebigen tragbaren oder Desktop-Computer eingerichtet werden, sofern dieser die folgenden Anforderungen erfüllt:

- Prozessor: Pentium II/266 MHz oder schneller
- Freie Festplattenkapazität: 4MB
- 64 MB RAM (128 MB oder mehr empfohlen)
- Microsoft Windows 98, ME, 2000 oder NT V4.0
- CD-ROM drive.

Für den **CP 1515 Manager** werden darüber hinaus benötigt:

- CP 1515

Für den **RLM Manager** müssen folgende Voraussetzungen erfüllt sein:

- Zugang zum LAN über
  1. CP 1515 oder
  2. Ethernet-Karte
- SIMATIC NET IWL Access Point RLM.
- Installation eines TCP/IP-Protokolls mit einer Winsock (Windows Sockets)-Schnittstelle. Die entsprechenden TCP/IP-Treiber befinden sich auf den Microsoft Windows-Installationsdisketten bzw. der CD-ROM.

3.3 Verwalten von Peer-to-Peer-Workgroups

Eine Peer-to-Peer-Workgroup besteht aus mehreren Stationen, die direkt miteinander kommunizieren, ohne Daten über das Access Point RLM zu bridgen.

Für Peer-to-Peer-Workgroups werden die Siemens SIMATIC NET IWL-Tools nicht benötigt. Weitere Informationen hierzu entnehmen Sie bitte der mit dem Produkt mitgelieferten Dokumentation "Industrial Ethernet Wireless LAN CP 1515".

3.4 Verwalten von Infrastruktur-Netzen

Die Konfigurierung der Access Points (RLMs) und die Überwachung des Funkverkehrs zwischen ausgewählten RLMs und Stationen in einem Infrastruktur-Netz wird in erster Line über die LAN-Administratorstation erfolgen, auf der der RLM Manager installiert ist.

Wenn Sie den CP 1515 Manager auf sämtlichen Stationen im Netz oder auf ausgewählten mobilen Stationen mit der PC Card CP 1515 installieren, können Sie die Verbindungsstrecke zwischen der mobilen Station und den nächstgelegenen Access Points (RLMs) überwachen.

3.4.1 Leitungsgebunden oder drahtlos?

Die Entscheidung für eine drahtlose oder leitungsgebundene LAN-Administratorstation zur Netzverwaltung hängt von den spezifischen Erfordernissen und Möglichkeiten ab.

Hierzu sollten Sie sich zunächst einmal überlegen, in welcher Weise die Verwaltung des Netzes erfolgen soll. Als Ausgangspunkte zum Konfigurieren und Überwachen von Stationen kommen in Frage:

- **Mobil** (zur Fehlersuche am physikalischen Standort einer Station): In diesem Fall wäre eine mobile, drahtlose LAN-Administratorstation am besten geeignet.

  Tool: RLM Manager und CP 1515 Manager
- **Ein zentraler Standort** (LAN-Administratorstation): In diesem Fall wäre eine leitungsgebundene LAN-Administratorstation vorzuziehen.

  Tool: RLM Manager

- **Ein Remote-Standort** mit Einwahl ins Netz über einen RAS- oder PPP-Einstiegspunkt per Modem

  Tool: RLM Manager

Bei der Entscheidung für eine leitungsgebundene oder drahtlose Station sollte außerdem die Größe des Netzes berücksichtigt werden. Zur Verdeutlichung:

- In größeren Netzen ist es unter Umständen praktischer, die einzelnen Stationen von einem zentralen Standort aus zu verwalten, so dass hier eher ein leitungsgebundener Administratorplatz in Frage kommt.
- Bei kleineren Netzkonfigurationen mit nur wenigen Access Points (RLMs) ist die Konfigurierung und Verwaltung über einen mobilen, drahtlosen Administratorplatz vermutlich am effizientesten.

Bei Verwendung eines drahtlosen Administratorplatzes gilt es folgendes zu beachten:

- Für den LAN-Administrator müssen die verschiedenen Bereiche des Drahtlos-Netzes gut zugänglich sein (z.B. zur Fehlersuche vor Ort).
- Für eine bestmögliche Positionierung der Access Points (RLMs) muss eine Standortprüfung vorgenommen werden.
- Das Access Point RLM lässt sich dabei auch remote über eine DFÜ-Verbindung konfigurieren und überwachen. Diese Funktion ist jedoch nur dann verfügbar, wenn von außen eine Zugangsmöglichkeit zum Netz besteht.

Natürlich können auch mehrere (leitungsgebundene und drahtlose) Stationen als LAN-Administratorstation eingerichtet werden, so dass in jeder Situation das entsprechende Tool zur Verfügung steht.

3.4.1.1 Leitungsgebundene Stationen

An einer leitungsgebundenen LAN-Administratorstation können Sie über das leitungsgebundene Backbone Access Points (RLMs) mit Hilfe des Tools RLM Manager konfigurieren und überwachen.

3.4.1.1.1 Konfiguration

Von einer leitungsgebundenen LAN-Administratorstation kann über das Backbone-Netz auf sämtliche Access Points (RLMs) zugegriffen werden. Die Access Points (RLMs) werden dabei anhand ihrer eindeutigen IP-Adresse identifiziert.

Umfasst die LAN-Architektur mehrere über Gateways oder Router miteinander verbundene Subnetze, ist zu beachten, dass sich die für die Erstkonfigurierung verwendete LAN-Administratorstation im selben Subnetz wie die Access Points (RLMs) befindet.

Sind die Access Points (RLMs) einmal eingerichtet und die jeweiligen IP-Adressen angemeldet, kann von jeder beliebigen Station über TCP/IP auf die Access Points (RLMs) zugegriffen werden.

Weitere Hinweise zur Konfigurierung der Access Point RLM entnehmen Sie bitte dem Abschnitt "Konfigurationsbeispiele" (Seite 50).

3.4.1.1.2 Überwachung

Beim Einsatz einer leitungsgebundenen LAN-Administratorstation besteht nicht die Möglichkeit, sich an den Standort von Stationen oder Access Points (RLMs) im Netz zu begeben, um deren Positionierung zu prüfen und ggf. anzupassen.

Allerdings können an einer leitungsgebundenen LAN-Administratorstation mit Hilfe der RLM Manager-Funktionen Remote Link Test und Remote-Statistik entsprechende Überwachungsmaßnahmen durchgeführt werden.

Mit Hilfe des RLM Manager können Sie Funkfrequenz-Verbindungen zwischen einem abgesetzten Access Point RLM und den am Radio Link Module angeschlossenen Stationen auf deren Funktion überprüfen. Weitere Hinweise zum Thema Überwachung entnehmen sie bitte dem Abschnitt "Überwachungs-Optionen" (Seite 107).

3.4.1.2 Drahtlose Stationen

An einer drahtlosen mobilen LAN-Administratorstation können Sie gleichermaßen den CP 1515 Manager wie auch den RLM Manager nutzen.

3.4.1.2.1 Überwachung

Zur Überwachung des Infrastruktur-Netzes stehen folgende Tools zur Verfügung:

- CP 1515 Manager
  1. Diagnose des CP 1515
  2. Protokollierung von Messdaten
  3. Site Monitor
  4. Link Test
- RLM Manager
  1. Systemdaten
  2. Remote Link Test
  3. Remote-Statistik

Weitere Hinweise zur Überwachung des Netzes entnehmen Sie bitte Kapitel 5 "Überwachen des SIMATIC NET IWL-Netzes" (Seite 73).

3.5 Installation der SIMATIC NET IWL-Software

3.5.1 CP 1515 Manager

Beim CP 1515 Manager handelt es sich um eine Diagnose-Tool, das nur auf IWL-Stationen einsetzbar ist. Damit das Programm CP 1515 Manager auf der LAN-Administratorstation ausführbar ist, muss die betreffende Station mit dem CP 1515 ausgerüstet sein.

Zum Installieren der CP 1515 Manager-Software gehen Sie folgendermaßen vor:

1. Legen Sie die SIMATIC NET IWL CD-ROM, die mit Ihrem IWL-Produkt ausgeliefert wurde, ins CD-Laufwerk.

   Falls Sie die Software aus dem Internet heruntergeladen haben, ziehen Sie bitte die Installationsanleitung aus dem Internet zu Rate.

2. Wird automatisch der CD-Browser aufgerufen, fahren Sie mit dem nächsten Punkt fort. Ansonsten gehen Sie wie folgt vor:

   - Klicken Sie in der Windows-Taskleiste auf die Schaltfläche **Start** und danach auf **Ausführen**.
   - Klicken Sie im Fenster Ausführen auf die Schaltfläche **Durchsuchen**.
   - Wählen Sie den Laufwerksbuchstaben des CD-ROM-Laufwerks, makieren Sie die Datei "setup.exe" und klicken Sie auf die Schaltfläche **Öffnen**.

- Klicken Sie im Fenster Ausführen auf die Schaltfläche **OK**. Daraufhin wird der CD-Browser gestartet.

3. Klicken Sie auf **RLM-, CP 1515-Manager** installieren
4. Klicken Sie auf **CP 1515-Manager** installieren.
5. Befolgen Sie die Anweisungen auf dem Bildschirm. Falls noch nicht vorhanden, wird im Windows Programm-Menü eine eigene Programmgruppe Siemens eingerichtet. Über diese Gruppe können Sie den CP 1515 Manager aufrufen.



HINWEIS:

Zuvor installierte Versionen der CP 1515 Manager-Software werden automatisch ersetzt.

Während der Installation werden Sie aufgefordert, ein Verzeichnis anzugeben, in dem die Programmdateien abgelegt werden sollen. Das Standardverzeichnis für die CP 1515 Manager-Software lautet:

C:\Programme\Siemens I-Gate\Clientmanager

Im vorliegenden Handbuch wird des Öfteren auf verschiedene Dateien verwiesen. Sofern nicht anders angegeben, befinden sich diese Dateien in dem o.g. Standardverzeichnis.

3.5.2 RLM Manager

Der RLM Manager kann sowohl auf drahtlosen als auch auf leitungsgebundenen Stationen installiert werden. Zur Installation des

Programms muss eine Station ausgewählt werden, auf der folgende Komponenten eingerichtet sind:

- NIC (Network Interface Card) zum Anschluss der Station an das Netz Bei der NIC-Karte kann es sich um einen beliebigen Typ handeln, einschließlich:
  1. CP 1515 (für drahtlose Stationen)
  2. Ethernet-Karte
- TCP/IP-Protokoll stack (siehe hierzu auch "Prüfen der TCP/IP-Einstellungen" (Seite 47)).

3.5.3 Installation des RLM Manager

Zum Installieren der RLM Manager-Software gehen Sie folgendermaßen vor:

1. Legen Sie die mit dem Produkt mitgelieferte CD-ROM im CD-ROM-Laufwerk des Computers ein, den Sie als LAN-Administratorstation festgelegt haben.

   Falls Sie die Software aus dem Internet heruntergeladen haben, ziehen Sie bitte die Installationsanleitung aus dem Internet zu Rate.
2. Wird automatisch der CD-Browser aufgerufen, fahren Sie mit dem nächsten Punkt fort. Ansonsten gehen Sie wie folgt vor:
   - Klicken Sie in der Windows-Taskleiste auf die Schaltfläche **Start** und danach auf **Ausführen**.
   - Klicken Sie im Fenster Ausführen auf die Schaltfläche **Durchsuchen**.

- Wählen Sie den Laufwerksbuchstaben des CD-ROM-Laufwerks, makieren Sie die Datei "setup.exe" und klicken Sie auf die Schaltfläche **Öffnen**.
- Klicken Sie im Fenster Ausführen auf die Schaltfläche **OK**. Daraufhin wird der CD-Browser gestartet.

3. Klicken Sie auf **RLM-, CP 1515-Manager** installieren
4. Klicken Sie auf **RLM-Manager** installieren.
5. Befolgen Sie die Anweisungen auf dem Bildschirm. Falls noch nicht vorhanden, wird im Windows Programm-Menü eine eigene Programmgruppe Siemens eingerichtet. Über diese Gruppe können Sie den RLM Manager zum Konfigurieren des Access Point RLM aufrufen.



HINWEIS:

Zuvor installierte Versionen der RLM Manager-Software werden automatisch ersetzt, wobei ggf. im Programmverzeichnis abgelegte andere Dateien hiervon nicht berührt werden. Haben Sie im RLM Manager-Programmverzeichnis beispielsweise Sicherungen von Access Point RLM-Konfigurationsdateien abgelegt, die sie mit einer älteren Version erstellt haben, so bleiben diese Dateien in unveränderter Form erhalten.

Während der Installation werden Sie aufgefordert, ein Verzeichnis anzugeben, in dem die Programmdateien abgelegt werden sollen. Das Standardverzeichnis für die RLM Manager-Software lautet:

C:\Programme\ORiNOCO\AP Manager

Im vorliegenden Handbuch wird des Öfteren auf verschiedene Dateien verwiesen. Sofern nicht anders angegeben, befinden sich diese Dateien in dem o.g. Standardverzeichnis.

3.5.3.1 Prüfen der TCP/IP-Einstellungen

Damit das Programm RLM Manager mit dem Access Point RLM kommunizieren kann, muss das Vernetzungsprotokoll TCP/IP eingerichtet sein. Beim erstmaligen Einrichten der Access Points (RLMs) müssen zunächst die TCP/IP-Einstellungen der LAN-Administratorstation und der Access Points (RLMs) überprüft werden.

Sie benötigen je eine IP-Adresse für den CP 1515 in Ihrer LAN-Administratorstation und für den Access Point RLM.

Es gibt zwei Wege um zu diesen IP-Adressen zu kommen:

- die CP1515- oder RLM IP-Adresse ist konfiguriert mit "Obtain an IP address automatically" via DHCP. Dann muß Ihr LAN-Administrator den DHCP-Server mit der MAC-Adresse von CP 1515 und RLM konfigurieren.
- Sie setzten die IP-Adresse von manuell. Dann müssen Sie sich IP-Adressen von ihrem LAN-Administrator zuteilen lassen (siehe Abschnitt "Über IP-Adressen und Subnetze" (Seite 257)).

Um festzustellen, ob das TCP/IP-Protokoll ordnungsgemäß installiert ist, gehen Sie bitte folgendermaßen vor:

1. Klicken Sie in der Windows-Taskleiste auf die Schaltfläche 

.
2. Führen Sie den Mauszeiger auf **Einstellungen** und klicken Sie anschließend auf **Systemsteuerung**.
3. Doppelklicken Sie im Fenster Systemsteuerung auf das Symbol **Netzwerk**.
4. Prüfen Sie, ob in der Liste der Netzwerkkomponenten für die LAN-Schnittstelle, über die auf den Access Point RLM zugegriffen werden soll (z.B. Ethernet karte oder CP 1515), das Protokoll TCP/IP **aufgeführt ist.**
   - Falls **Ja**, schließen Sie alle Fenster über die Schaltfläche **Abbrechen** und fahren Sie wie unter "Konfigurationsbeispiele" (Seite 50) beschrieben fort.
   - Falls **Nein**, gehen Sie bitte folgendermaßen vor:
     a. Klicken Sie auf die Schaltfläche **Hinzufügen**.
     b. Wählen Sie in der Liste der Komponenten **Protokoll** und klicken Sie auf die Schaltfläche **Hinzufügen**.
     c. Wählen Sie das Protokoll TCP/IP aus.
     d. Arbeitet das Netzwerk nicht mit IP-Adressierung, aktivieren Sie das Kontrollkästchen **IP-Adresse festlegen**.

        Damit wird der DHCP-Mechanismus deaktiviert, über den dem LAN-Adminstratorplatz in Netzen mit einem DHCP-Server automatisch eine IP-Adresse zugewiesen wird.

e. Geben Sie im Feld **IP-Adresse** einen benutzerdefinierten Wert im Format **153.69.254.xxx** ein, wobei xxx ein beliebiger numerischer Wert zwischen 1 und 253 sein kann.

   Werden mehrere LAN-Administratorplätze eingerichtet, achten Sie darauf, dass Sie jeder Station einen anderen Wert geben.

f. Geben Sie im Feld Subnetmask den Wert **255.255.255.0** ein.

g. Klicken Sie zum Bestätigen Ihrer Eingaben auf die Schaltfläche **OK** und befolgen Sie die Anweisungen auf dem Bildschirm.

5. Wenn Sie zum Neustarten des Computers aufgefordert werden, wählen Sie **Ja**.

Nach dem Wiederhochlauf des Computers können Sie das Access Point RLM gemäß den in "Konfigurationsbeispiele" (Seite 50) beschriebenen Beispielen konfigurieren.

3.6 Konfigurationsbeispiele

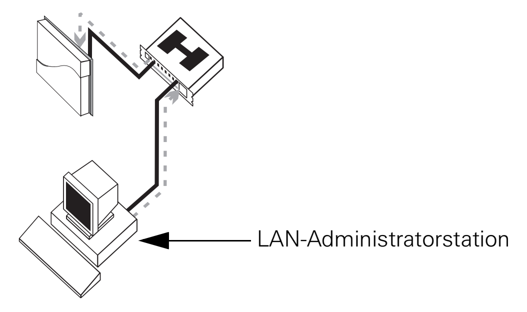
Im vorherigen Abschnitt wurden Kriterien für die Wahl einer leitungsgebundenen oder drahtlosen LAN-Administratorstation behandelt. Der vorliegende Abschnitt befasst sich mit Merkmalen der beiden Typen und gibt an, ob am Computer bzw. "Desktop-Arbeitsplatz" noch weitere Änderungen vorzunehmen sind.

3.6.1 Leitungsgebundene LAN-Administratorstation

Beim Einsatz einer leitungsgebundenen LAN-Administratorstation haben Sie folgende Optionen zum Konfigurieren der Access Points (RLMs):

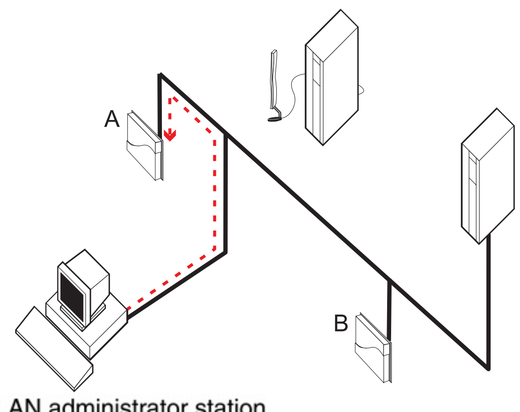
- Eine "Desktop-Arbeitsplatz"-Anordnung, bei der der Computer wie in Abbildung 5 Leitungsgebundener Zugang über eine Kabel-Direktverbindung dargestellt, über einen Hub/Switch oder einfach ein gekreuztes TP-Cord mit dem Access Point RLM verbunden ist.

Abbildung 5 Leitungsgebundener Zugang über eine Kabel-Direktverbindung



- Eine leitungsgebundene Ethernet-LAN-Verbindung wie in Abbildung 6 Leitungsgebundener Zugang über eine Netzwerkverbindung dargestellt

Abbildung 6 Leitungsgebundener Zugang über eine Netzwerkverbindung



Die Wahl einer leitungsgebundenen LAN-Administratorstation wird in folgenden Fällen empfohlen:

- Die Access Points (RLMs) sollen von einem festen zentralen Standort aus verwaltet werden.
- Die Access Points (RLMs) werden an entfernten Standorten installiert, die über TCP/IP erreichbar sind.

Bei dem Beispiel in Abbildung 6 kann die LAN-Administratorstation über das leitungsgebundene Backbone-Netzwerk auf die beiden Access Points (RLMs) **A** und **B** zugreifen.

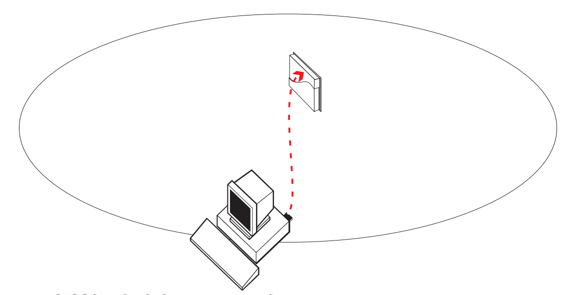
- Arbeiten die Access Points (RLMs) noch mit der werksseitig vorgegebenen Konfiguration, können die Radio Link Modules anhand ihrer Ethernet MAC-Adresse identifiziert werden - vorausgesetzt, die Access Points (RLMs) befinden sich im selben Subnetz wie die LAN-Administratorstation (d.h. es sind keine Router zwischen die LAN-Administratorstation und das Access Point RLM geschaltet).
- Wurde jedem Access Point RLM eine eindeutige IP-Adresse zugewiesen, so sollte jeder Access Point RLM von jedem Punkt des Netzes über die betreffende IP-Adresse erreichbar sein.

Werden neue Access Points (RLMs) mit den Standardeinstellungen installiert, so wird empfohlen, die Radio Link Modules einzeln mit dem in Abbildung 5 Leitungsgebundener Zugang über eine Kabel-Direktverbindung dargestellten "Desktop-Arbeitsplatz"-Szenario zu konfigurieren. Auf diese Weise können Sie jedem Gerät eine eindeutige IP-Adresse zuweisen, bevor die Geräte an die Netzwerkinfrastruktur angeschlossen werden.

3.6.2 Drahtlose LAN-Administratorstation

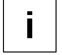
Auf einer drahtlosen mobilen LAN-Administratorstation können Sie den RLM Manager in Verbindung mit dem Tool CP 1515 Manager benutzen.

Abbildung 7 Drahtloser Zugang über Direktverbindung



Beim Einsatz einer drahtlosen LAN-Administratorstation haben Sie folgende Optionen zum Konfigurieren der Access Points (RLMs):

- Direkt über eine drahtlose Punkt-zu-Punkt-Verbindung wie in Abbildung 7 Drahtloser Zugang über Direktverbindung dargestellt oder
- Indirekt über eine drahtlose Punkt-zu-Punkt-Verbindung zu einem anderen Access Point RLM, das den Zugang zum "Ziel"-Access Point RLM wie in Abbildung 8 Drahtloser Zugang über eine indirekte Verbindung dargestellt über ein Backbone herstellt.



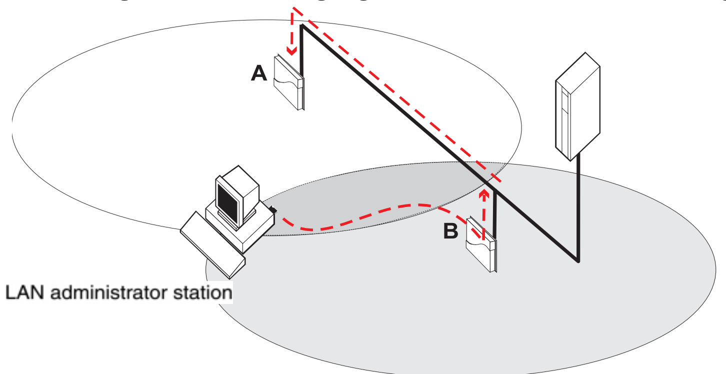
HINWEIS:

Genauso, wie bei einem leitungsgebundenen Netz für eine ordnungsgemäße Verbindung sichergestellt sein muss, dass sämtliche Kabel richtig angeschlossen sind, muss bei einem Wireless-LAN folgendes gewährleistet sein:

- Die LAN-Administratorstation befindet sich innerhalb der Funkreichweite des "Ziel"-Access Point RLM und
- Die Einstellungen der Drahtlos-Netzschnittstelle entsprechen den Parameterwerten des oder der Access Point RLM(s).

Bei Verwendung der in Abbildung 7 Drahtloser Zugang über Direktverbindung dargestellten Konfiguration sollte die drahtlose Netzwerk-Schnittstelle der LAN-Administratorstation so konfiguriert sein, dass deren Einstellungen denen des "Ziel"-Access Point RLM entsprechen.

Abbildung 8 Drahtloser Zugang über eine indirekte Verbindung



Bei dem in Abbildung 8 Drahtloser Zugang über eine indirekte Verbindung dargestellten Szenario sollte die drahtlose Netzwerk-Schnittstelle der LAN-Administratorstation so konfiguriert sein, dass deren Einstellungen denen des Access Point RLM **B** entsprechen.

- Das in Abbildung 7 Drahtloser Zugang über Direktverbindung dargestellte Szenario bietet sich an, wenn nacheinander mehrere Access Points (RLMs) mit den Standardeinstellungen konfiguriert werden sollen.
- Das Szenario in Abbildung 8 Drahtloser Zugang über eine indirekte Verbindung eignet sich besonders, wenn in einem bestehenden Netzwerk zusätzliche Access Points (RLMs) eingerichtet werden sollen oder wenn sich die Administrator-Station außerhalb der Funkreichweite des "Ziel"-Access Point RLM befindet.

In beiden Fällen werden die Access Points (RLMs) anhand ihrer eindeutigen IP-Adresse identifiziert.

3.7 Deinstallieren der SIMATIC NET IWL-Software

Möchten Sie die SIMATIC NET IWL-Software von der LAN-Administratorstation entfernen, verwenden Sie die Funktion "Hinzufügen/Entfernen" in Windows.

Zum Deinstallieren der SIMATIC NET IWL-Software gehen Sie folgendermaßen vor:

1. Klicken Sie in der Windows-Taskleiste auf die Schaltfläche **Start**.
2. Führen Sie den Mauszeiger auf **Einstellungen** und klicken Sie anschließend auf **Systemsteuerung**.
3. Doppelklicken Sie im Fenster Systemsteuerung auf das Symbol **Software**.
4. Markieren Sie das Programm, das deinstalliert werden soll, und klicken Sie auf die Schaltfläche **Hinzufügen/Entfernen**.

Über die Option **Hinzufügen/Entfernen** werden lediglich die Programmdateien gelöscht. Haben Sie im Verzeichnis mit den Programmdateien z.B. Log-Dateien abgelegt, so bleiben diese erhalten.

4 Einfache Netzkonfigurationen

4.1 Einführung

Das vorliegende Kapitel beschreibt die Konfigurierung eines SIMATIC NET IWL-Netzwerks für:

- Peer-to-Peer-Workgroups und
- Infrastruktur-Netzwerke

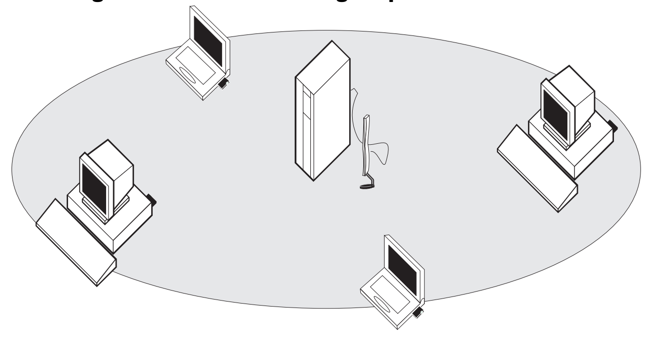
4.1.1 Peer-to-Peer-Workgroups

Eine Peer-to-Peer-Workgroup besteht aus mehreren IWL-Stationen, die direkt miteinander kommunizieren, ohne Daten über das RLM zu bridgen (siehe Abbildung 9 Peer-to-Peer-Workgroup).

Zum Einrichten einer Peer-to-Peer-Workgroup, die mit Standard-Protokollen arbeitet, gehen Sie folgendermaßen vor:

- Stellen Sie bei allen Stationen ein, dass diese eine Verbindung zu einer Peer-to-Peer-Workgroup herstellen sollen.
- Stellen Sie bei allen Stationen den selben Netzwerknamen ein.
- Stellen Sie bei allen Stationen den selben Chiffrierschlüssel ein.

Abbildung 9 Peer-to-Peer-Workgroup



4.1.2 Infrastruktur-Netzwerke

Mit Hilfe von Access Points (RLMs) und den Produkten der Familie SIMATIC NET IWL können Sie eine unbegrenzte Zahl von Netzwerk-Konfigurationen realisieren. Der Übersichtlichkeit halber ist das übrige Kapitel daher in drei Abschnitte gegliedert, in denen erläutert wird, wie Sie Ihr Netzwerk grundsätzlich in Betrieb nehmen können.

- Die Anleitungen unter Konfigurieren von Infrastruktur-Netzwerken (Seite 62) sind für die meisten Netzwerk-Umgebungen anwendbar.
- Komplexere Konfigurationen sind in Kapitel 8 Erweiterte Netzwerkkonfiguration (Seite 212) beschrieben.

- Im Abschnitt Erweiterte Parameter (Seite 213) finden Sie Hinweise, wie Sie die Konfiguration des Radio Link Module individuell an die Erfordernisse des Netzwerks anpassen können.
- Unter Konfiguration großer Netzwerke (Seite 242) ist erläutert, wie sich die RLM-Hardware effizienter verwalten lässt.

4.1.2.1 Voraussetzungen

Um die Access Points (RLMs) verwalten zu können, müssen Sie zunächst jedem RLM im Netz eine eindeutige IP-Adresse zuweisen.

Die Manager-Station muss ebenfalls eine IP-Adresse haben. Die TCP/IP-Verbindung dieser Station sollte entweder:

- auf das selbe Subnetz führen, in dem sich die Access Points (RLMs) befinden (siehe Beschreibung in Einfache Infrastrukturen (Seite 28)), oder
- über Router, Gateways oder eine andere LAN-Verbindung, die TCP/IP unterstützt, den Zugang auf das Subnetz der Access Points (RLMs) erlauben.

4.2 Konfigurieren von Infrastruktur-Netzwerken

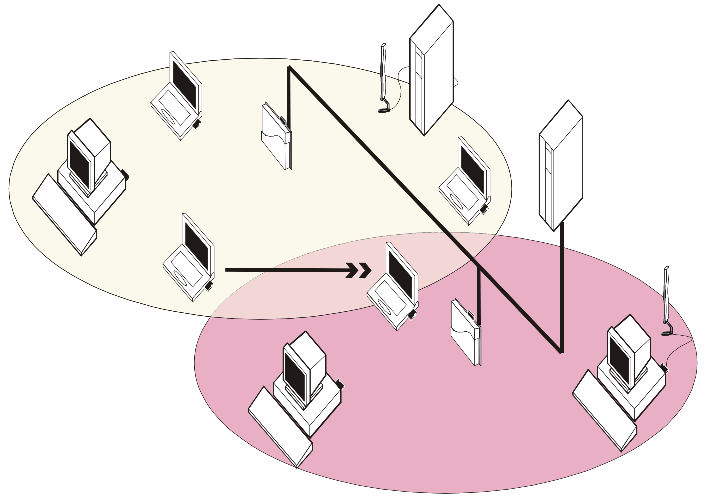
4.2.1 Einfache Konfigurationen

4.2.1.1 Einführung

Der vorliegende Abschnitt beschreibt in vier Schritten, wie die Access Points (RLMs) zu konfigurieren sind, damit über diese drahtlose (mobile) Stationen in einer Roaming-Netzwerkumgebung versorgt werden können.

In dem Beispiel in Abbildung 10 Basic Access-Netzwerk werden die einzelnen Funkzellen jeweils von einem eigenen RLM versorgt, bei dem "Access Point Services" eingestellt ist. Die Access Points (RLMs) verwenden dabei alle den selben Netzwerknamen.

Abbildung 10 Basic Access-Netzwerk



Beim Anschließen drahtloser Stationen an das SIMATIC NET IWL-Netz muss für diese jeweils der selbe Netzwerkname wie für das Radio Link Module eingerichtet werden.

Befolgen Sie beim Konfigurieren der IWL-Stationen die Anweisungen der Dokumentation, die mit dem Drahtlos-Client- Adapter CP 1515 mitgeliefert wurde.

Zum Installieren und Einrichten des RLM gehen Sie folgendermaßen vor:

1. Installieren Sie die Radio Link-Modul-Hardware$_1$.

2. Stellen Sie mit dem Programm RLM Manager eine Verbindung zum RLM her.
3. Stellen Sie den Netzwerknamen ein und speichern Sie die Konfiguration im Radio Link Module.
4. Erstellen Sie eine Sicherungsdatei der neuen Konfigurationseinstellungen (nicht zwingend notwendig, aber empfehlenswert).

Wiederholen Sie die Schritte 2 bis 4 für sämtliche zu installierende Access Points (RLMs).

4.2.1.2 Schritt 1 - Installieren des Access Point RLM

Hinweise zur Installation der RLM-Hardware entnehmen sie bitte der Dokumentation, die mit dem RLM mitgeliefert wurde.

4.2.1.3 Schritt 2 - Herstellen einer Verbindung zum Access Point RLM

Um eine Verbindung zu einem Radio Link-Modul herstellen zu können, müssen Sie das jeweilige Radio Link Module über dessen IP-Adresse ansprechen.

- Ist im Netz ein BOOTP- oder DHCP-Server vorhanden, werden die IP-Adressen automatisch vergeben (nähere Angaben hierzu finden Sie unter BOOTP und DHCP (Seite 258)).

1. Je nachdem, für welche der in Einrichten der LAN-Administratorstation (Seite 34) genannten Konfigurationen Sie sich entschieden haben, werden Sie die Access Points (RLMs) entweder zunächst an Ihrem Arbeitsplatz installieren und einzeln konfigurieren, oder Sie lassen die Access Points (RLMs) direkt an ihrem vorgesehenen Standort installieren und konfigurieren diese dann über eine Netzwerkverbindung.

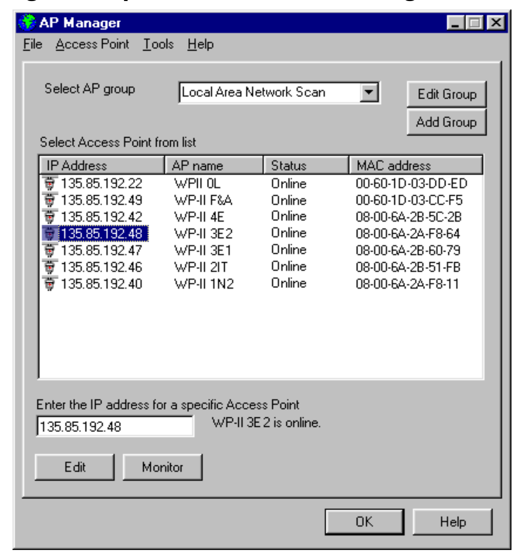
- In den Fällen, wo die IP-Adresse nicht automatisch zugewiesen wird, lautet die werksseitig voreingestellte IP-Adresse 153.69.254.254.

  Diese werksseitig vorgegebene IP-Adresse (153.69.254.254) muss bei der Erstkonfiguration abgeändert werden.

Zum Herstellen einer Verbindung zum RLM gehen Sie folgendermaßen vor:

1. Starten Sie das Programm RLM Manager.
2. Wählen Sie das zu konfigurierende Radio Link-Modul aus der Liste aus oder geben Sie im Feld **Enter the IP address for a specific Access Point** die entsprechende IP-Adresse ein (siehe Abbildung 11 Hauptfenster des RLM Manager).
   - Ein neues Radio Link-Modul wird durch ein spezielles Symbol gekennzeichnet.
   - In der Liste werden sämtliche Access Points (RLMs) angezeigt, die sich im selben IP-Subnetz wie die Manager-Station befinden (siehe hierzu auch Ändern der Konfiguration (Seite 253)).
   - Um auf Access Points (RLMs) in einem anderen Subnetz oder über eine DFÜ-Verbindung zuzugreifen, geben Sie im Feld **Enter the IP address for a specific Access Point** die jeweilige IP-Adresse ein.

Abbildung 11 Hauptfenster des RLM Manager



3. Klicken Sie auf die Schaltfläche **Edit**.
   - Hat das von Ihnen ausgewählte RLM noch die werksseitig vorgegebene IP-Adresse 153.69.254.254, werden Sie zu Ändern der IP-Adresse aufgefordert.

a. Geben Sie für das Radio Link-Modul im Feld Access Point **IP Address** eine eindeutige IP-Adresse ein.

b. Notieren Sie die IP-Adresse in der **RLM-Konfigurationstabelle** unter A “Startkonfiguration”.

4. Geben Sie das Read/Write-Passwort ein und klicken Sie auf **OK** (das Default-Passwort lautet "public").

   - Wurde das RLM gefunden und es wurden die richtigen Passwörter eingegeben, erscheint ein neues Fenster mit Parametern (auf Registerkarten) zum Ändern der Konfiguration (siehe Abbildung 12 Registerkarte Wireless Interfaces im Fenster RLM Manager).
   - Wurde das Radio Link-Modul im Netzwerk nicht gefunden bzw. die Konfiguration nicht eingelesen, oder es wurde das falsche Passwort eingegeben, so erscheint die Meldung "**Invalid password**". Klicken Sie auf **OK**, um wieder zum Hauptfenster des RLM Manager zu gelangen und wiederholen Sie Ihre Eingaben.

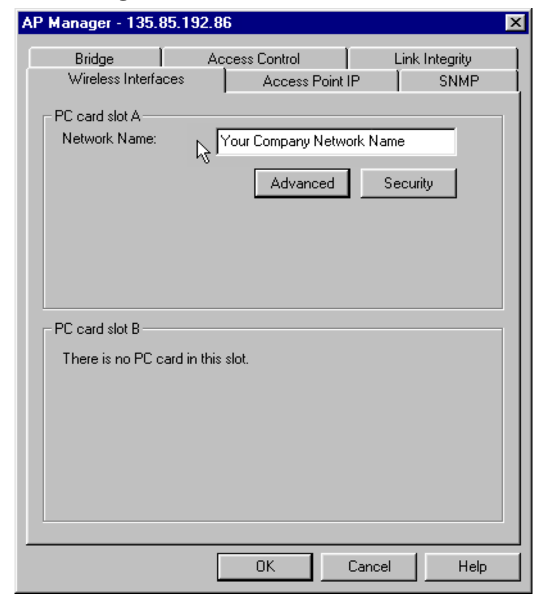
Sie können nun die Konfigurationseinstellungen des RLM ändern.

4.2.1.4 Schritt 3 - Einstellen des Netzwerknamens und Speichern der Konfiguration

Es wird empfohlen bei der Installation des SIMATIC NET IWL-Netzes die Standardeinstellungen der Wireless-LAN-Schnittstellen abzuändern. Zwar funktioniert das Radio Link-Modul auch mit den werksseitig vorgegebenen Werten, aber durch Abändern der Parameter auf eindeutige Werte lässt sich das Netzwerk klarer von ggf. vorhandenen benachbarten Netzwerken abgrenzen.

1. Wählen Sie die Registerkarte **Wireless Interfaces** (siehe Abbildung 12 Registerkarte Wireless Interfaces im Fenster RLM Manager).
2. Wählen Sie den Steckplatz am RLM (**PC Card slot A** oder **B**, der die zu konfigurierende PC-Karte enthält.

Abbildung 12 Registerkarte Wireless Interfaces im Fenster RLM Manager



3. Geben Sie für die Schnittstelle im Feld **Network Name** eine Bezeichnung für den Dienst ein:

Beim Netzwerknamen kann es sich um eine beliebige alphanumerische Zeichenfolge mit maximal 32 Stellen und den Zeichen "a" bis "z", "A" bis "Z" und "0" bis "9" handeln.

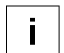
Es sollte für sämtliche drahtlose Netzwerk-Schnittstellen, die drahtlose Stationen im Netz versorgen, der selbe Netzwerkname eingestellt werden.

Mit Hilfe des Netzwerknamens lassen sich die eigenen Access Points (RLMs) von Access Points (RLMs) eines benachbarten Netzwerkes unterscheiden.

Angaben zu den übrigen Schnittstellen-Parametern (z.B. den Schaltflächen **Advanced** und **Security**) finden Sie im Abschnitt Erweiterte Netzwerkkonfiguration (Seite 212).

4. Nach Abschluss der Änderungen klicken Sie auf **OK**, um die Konfiguration im Access Point RLM zu speichern und wieder zum Hauptfenster des RLM Manager (siehe Abbildung 11 Hauptfenster des RLM Manager) zu gelangen.

   In diesem Stadium werden die IP-Adresse und andere Einstellungen im flüchtigen Speicher des RLM abgelegt.



HINWEIS:

Nach Abspeichern der Konfiguration im Radio Link-Modul (durch Anklicken der Schaltfläche **OK**) wird das RLM automatisch neu gestartet.

Damit ist die Grundkonfiguration des RLM abgeschlossen. Diese Grundkonfiguration funktioniert in den meisten Vernetzungssituationen tadellos. Es wird empfohlen, gemäß Beschreibung unter Schritt 4 - Erstellen

einer Sicherungsdatei der Konfiguration (Seite 72) eine Sicherungsdatei dieser Konfiguration zu erstellen.

Angaben zu erweiterten Parametereinstellungen finden Sie im Abschnitt Erweiterte Netzwerkkonfiguration (Seite 212).

4.2.1.5 Schritt 4 - Erstellen einer Sicherungsdatei der Konfiguration

Es wird empfohlen, immer eine Sicherungsdatei der neuen Konfiguration zu erstellen, wenn die Konfiguration des Access Point RLM geändert wurde. Mit Hilfe dieser Datensicherung können Sie in den folgenden Fällen die Konfiguration des Radio Link-Moduls rasch wiederherstellen:

- Nach einem Ausfall des Access Point RLM
- Zur Wiederherstellung der Original-Konfiguration nach Austausch eines RLM (z.B. nach einer Reparatur)
- Nach Ausführung eines erzwungenen Reloads (siehe hierzu Erzwungener Neustart (Seite 275)).

Zum Erstellen einer Sicherungsdatei gehen Sie folgendermaßen vor:

1. Starten Sie das Programm RLM Manager.
2. Wählen Sie das RLM, für das eine Sicherungsdatei erstellt werden soll.
3. Wählen Sie im Access Point-Menü die Option **Download Config File**.
4. Geben Sie nach entsprechender Aufforderung einen Dateinamen ein, anhand dessen sich die Datei problemlos dem jeweiligen Radio Link-Modul zuordnen lässt.
5. Notieren Sie den Dateinamen und den Installationsort des RLM in der "Access Point RLM-Konfigurationstabelle" unter Startkonfiguration (Seite 260).

Zu Installation und Konfigurierung weiterer Access Points (RLMs) siehe Schritt 1 - Installieren des Access Point RLM (Seite 64).

5 Überwachen des SIMATIC NET IWL-Netzes

5.1 Einführung

Nachdem das Netzwerk fertig konfiguriert und installiert ist, können Sie mit Hilfe der SIMATIC NET IWL-Tools:

- das Netzwerk auf seine Performance überprüfen
- die optimale Position für Access Point RLMs und drahtlose Stationen ermitteln

Es wird empfohlen, die Performance des Netzwerks regelmäßig zu überprüfen, da sich diese infolge des Umzugs von IWL-Stationen, durch Einziehen oder Umstellen von Trennwänden in Räumen oder durch Installation von Geräten, die die Funkkommunikation stören können, verändern kann.

5.1.1 SIMATIC NET IWL-Tools

Die Software-Suite SIMATIC NET IWL enthält zwei Tools, mit deren Hilfe sich das Netzwerk überwachen lässt:

- CP 1515 Manager
- RLM Manager

5.1.1.1 CP 1515 Manager

Der CP 1515 Manager kann zur Überprüfung der Funkverbindungsqualität im Netz von einem beliebigen Standort aus verwendet werden. Das Programm bietet folgende Funktionen:

- Dynamische Auswertungen der Funkübermittlung mit dem Radio Link-Modul, in dessen Bereich sich die Überwachungs-Station befindet
- Anzeige der Ergebnisse von Link Test-Messungen mit dem Access Point RLM, der der CP 1515 Manager-Station am nächsten ist

Beim CP 1515 Manager handelt es sich um ein Tool für den mobilen Einsatz, das nur im Zusammenhang mit einem CP 1515 (z.B. auf einem Notebook-Computer) lauffähig ist.

5.1.1.2 RLM Manager

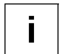
Der RLM Manager ist für die Überwachung des Netzwerks von einem zentralen Standort, z.B. der LAN-Administratorstation, ausgelegt.
Mit Hilfe dieses Tools können Sie Messergebnisse für die Verbindung zwischen einem (fernen) RLM und einer an dem ausgewählten RLM angeschlossenen Station ausgeben.

Das Tool RLM Manager ist sowohl auf leitungsgebundenen Stationen (Ethernet) als auch auf IWL-Stationen lauffähig. Für die Durchführung von Messauswertungen muss die LAN-Administratorstation an der Netzwerk-Infrastruktur angeschlossen sein, damit ein Zugang zum Access Point RLM über TCP/IP möglich ist.

5.1.2 Welches ist das richtige Tool?

Ob Sie nun den CP 1515 Manager oder den RLM Manager verwenden, hängt in erster Linie davon ab, ob Messauswertungen ortsunabhängig oder von einem zentralen Standort aus erfolgen sollen bzw. können.

Sowohl der CP 1515 Manager als auch der RLM Manager bieten Protokollierungsfunktionen, mit denen Messdaten für eine nachträgliche Auswertung oder für Vergleiche mit früheren Messungen gespeichert werden können. Sie können die gespeicherten Log-Dateien mit einem ASCII-Editor ansehen oder die Daten in Standard-Tabellenkalkulations- oder Datenbank-Anwendungen importieren.



HINWEIS:

Alternativ hierzu können Sie mit dem Programm RLM Manager die Funkverbindungsqualität von Drahtlos-Systemen über Radio Link-Module überwachen (siehe Fenster Remote Link Test (Seite 112)).

Die Produkte der Familie SIMATIC NET IWL sind für den Betrieb mit sämtlichen Drahtlos-LAN-Produkten ausgelegt, die mit der Direktsequenz-Funktechnologie gemäß dem Standard IEEE 802.11 arbeiten. Das mit dem nichtlizenzierten 2,4 GHz-Band arbeitende SIMATIC NET IWL-System erlaubt eine Übertragung durch Wände und Fußböden hindurch, so dass der Benutzer den Standort im Netz beliebig wechseln kann, ohne dass die Verbindung zum Netz abbricht.

Die SIMATIC NET IWL-Hardware kann mit Drahtlos-LAN-Produkten anderer Hersteller, die der IEEE 802.11 entsprechen, kommunizieren.

Dagegen ist die Software-Suite SIMATIC NET IWL unter Umständen nicht immer zusammen mit Fremdhersteller-Produkten einsetzbar, und zwar aus folgenden Gründen:

- Im Standard IEEE 802.11 für drahtlose LANs sind keine Normen für Diagnose- und Management-Tools festgelegt, so dass die einzelnen Hersteller möglicherweise jeweils eigene Tools für die Konfiguration und das Management von drahtlosen Netzwerken gemäß IEEE 802.11 konzipiert haben.
- Die Software-Suite SIMATIC NET IWL bietet eine umfangreiche Palette von Tools zur Überwachung und Auswertung verschiedenster Diagnosezähler.

  Für einige dieser Tools sind Zusatzfunktionen in der Hardware erforderlich, die von den Produkten der Familie SIMATIC NET IWL standardmäßig unterstützt werden, von den Produkten anderer Hersteller unter Umständen jedoch nicht.

Wenn Abfragen der Verbindungsqualität oder Konfigurationsparameter von Fremdhersteller-Produkten mit der Software-Suite SIMATIC NET IWL nicht möglich sein sollten, schlagen Sie bitte in der Dokumentation zum Fremdhersteller-Produkt nach.

5.2 Einsatz des CP 1515 Manager

5.2.1 Überwachungs-Optionen

Der CP 1515 Manager bietet vier verschiedene Überwachungs-Optionen:

- PC Card CP 1515-Diagnose (siehe Diagnose Card (Seite 104))
- Link Test (siehe Fenster Link Test (Seite 80))
- Site Monitor (siehe Fenster Site Monitor (Seite 88))
- Protokollierung von Messdaten (siehe Protokollierung von Messdaten (Seite 100))

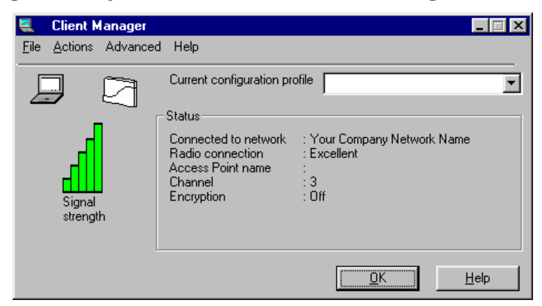
Die Optionen Site Monitor, Link Test und Protokollierung von Messdaten stehen nur dann zur Verfügung, wenn der CP 1515 Manager im Modus "Advanced" installiert wurde (siehe hierzu auch CP 1515 Manager (Seite 18)).

Starten des Tools CP 1515 Manager:

1. Das Programm CP 1515 Manager wird beim Starten von Windows automatisch mit gestartet. Dabei wird das CP 1515 Manager-Symbol in der Windows-Taskleiste eingeblendet. Sollte das Programm nicht ausgeführt werden, gehen Sie wie folgt vor:
   - Klicken Sie in der Windows-Taskleiste auf die Schaltfläche **Start**.
   - Wählen Sie **Programme** und klicken Sie die Programmgruppe **Siemens I-GATE** an.
   - Wählen Sie anschließend **Client Manager**, um das Programm CP 1515 Manager zu starten.

2. Klicken Sie in der Taskleiste auf das Symbol CP 1515 Manager , um das in CP 1515 Manager dargestellte Hauptfenster der Abbildung 13 Hauptfenster des CP 1515 Manager aufzurufen.

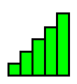
Abbildung 13 Hauptfenster des CP 1515 Manager



Im Hauptfenster des CP 1515 Manager werden die wichtigsten Daten zur Bewertung der Netzverbindung der SIMATIC NET IWL-Station angezeigt, nämlich:

- Der Name des Netzwerks, an dem die Station angeschlossen ist ("Peer-to-Peer" im Falle einer Peer-to-Peer-Workgroup oder der Netzwerkname der RLM-Infrastruktur, z.B. "Your company network name")
- Die Qualität der Funkverbindung zum Netzwerk:
  - Excellent (sehr gut)
  - Good (gut)
  - Marginal (im Grenzbereich)
  - Poor (schlecht) oder

- Out of range (außerhalb des abgedeckten Funkbereichs)



Die Qualität der Funkverbindung wird darüber hinaus durch eine Farbsymbolik angezeigt. Die einzelnen Farben bedeuten jeweils:

- Grün: Sehr gute oder gute Verbindung
- Gelb: Verbindungsqualität im Grenzbereich
- Rot: Schlechte Verbindung
- Rot mit Fehlersymbol: Keine Verbindung

- Der Name des Radio Link-Moduls, mit dem der drahtlose Mobil-Computer momentan verbunden ist
- Der Kanal, über den die Verbindung erfolgt
- Verschlüsselung: ein / aus

Konnte der CP 1515 Manager keine Netzverbindung herstellen, erscheint im Fenster eine der folgenden Hinweismeldungen:

- **No wireless network card driver present** - die Station konnte den SIMATIC NET IWL-Treiber nicht erkennen. Prüfen Sie in diesem Fall, ob der CP 1515 ordnungsgemäß angeschlossen ist und ob die Station richtig konfiguriert wurde.
- **Out of range** - Sie befinden sich außerhalb der Funkreichweite des Netzwerks, für das die Station konfiguriert wurde.
- **Searching for initial connection to network: Network Name** - das Netzwerk mit dem Namen Network Name kann nicht gefunden werden.

Ausführlichere Informationen erhalten Sie mit den unter Überwachungs-Optionen (Seite 77) beschriebenen Überwachungs-Optionen.

Vom Hauptfenster des CP 1515 Manager (siehe Abbildung 13 Hauptfenster des CP 1515 Manager) können Sie außerdem eine Reihe von Menüpunkten aufrufen. Diese werden in den nachfolgenden Absätzen beschrieben.

Falls Probleme beim Herstellen einer Verbindung zum Netzwerk auftreten sollten:

- Klicken Sie auf die Schaltfläche **Hilfe** oder drücken Sie die Taste F1 zu Hinweisen zur Problembehebung.
- Schlagen Sie mögliche Lösungen unter B “Problembehandlung” nach.

5.2.2 Fenster Link Test

Mit der Option Link Test können Sie in drahtlosen Umgebungen in geschlossenen Räumen ausführliche Messauswertungen zwischen der CP 1515 Manager-Station und einem bestimmten Testpartner vornehmen. Je nach Art des drahtlosen Netzwerks, mit der die CP 1515 Manager-Station verbunden ist, kann es sich beim Testpartner um folgende Geräte handeln:

- Das RLM, wenn die CP 1515 Manager-Station an einem "Infrastruktur-Netzwerk" angeschlossen ist (siehe Kapitel 2 Drahtlos-Konfigurationen)

  Bei diesem Netzwerktyp können Sie keinen anderen Link Test-Partner auswählen; beim Roaming im drahtlosen Netzwerk wechselt der Link Test-Partner immer dann, wenn mit einem anderen RLM eine bessere Übermittlungsqualität gegeben ist.
- Die drahtlose Station, wenn die CP 1515 Manager-Station an eine Peer-to-Peer-Workgroup angeschlossen ist (siehe Kapitel 2 Drahtlos-Konfigurationen

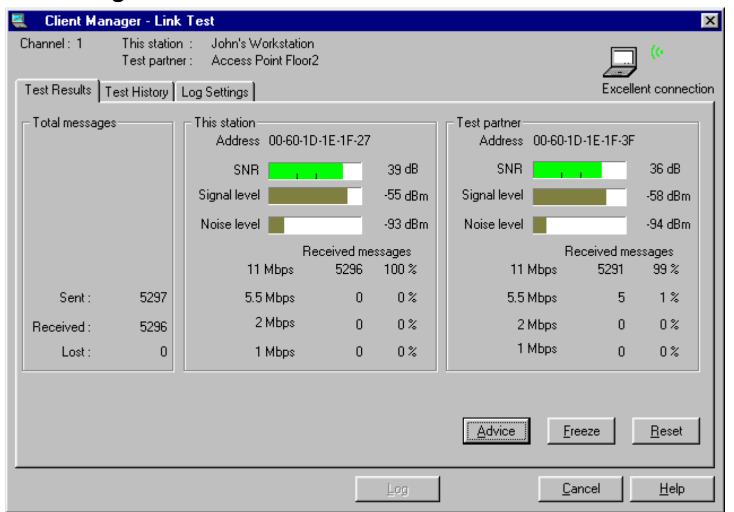
Bei diesem Netzwerktyp können Sie den Link Test-Partner aus einer Liste von Stationen auswählen, die in dem unabhängigen Netzwerk zur Verfügung stehen, das über den selben Netzwerknamen identifiziert wird wie die CP 1515 Manager-Station.

Zum Starten des Link Tests wählen Sie im Hauptfenster des im Menü CP 1515 Manager Advanced die Option **Link Test.** Hierauf erscheint das in Abbildung 14 Fenster Link Test dargestellte Fenster.

Im oberen Teil des Fensters Link Test erscheinen folgende Informationen:

- Der Funkkanal, über den die beiden Geräte kommunizieren
- Der Name des eigenen Computers (This Station)
- Der Name des Link Test-Partners (Test Partner) und
- Die Verbindungsqualität

Abbildung 14 Fenster Link Test



Im Fenster "Link Test" stehen Ihnen drei Optionen zur Auswertung der Link Test-Daten zur Verfügung:

- **Test results** - diese Option liefert Messergebnisse zum Link Test.
- **Test history** - diese Option liefert graphische Darstellungen zur Link-Qualität.
- **Log Settings** - hier lassen sich Parameter zur Erfassung von Testergebnissen für spätere Auswertungen einstellen.

5.2.2.1 Registerkarte Test Results

Über die Registerkarte Test Results rufen Sie ein Fenster auf, in dem die Ergebnisse des Link Tests anhand folgender Indikatoren angezeigt werden:

- Signal to noise ratio (SNR) (Störabstand)
- Received Messages (empfangene Meldungen)

5.2.2.1.1 Signal to Noise Ratio (SNR)

Der Wert Signal to Noise Ratio (SNR, Störabstand) zeigt die Verbindungsqualität der Funkstrecke zwischen der eigenen Station und dem Link Test-Partner an. Dieser Indikator wird laufend gemäß dem tatsächlichen Zustand der Funkstrecke aktualisiert.

Die einzelnen Farben der SNR-Anzeige stehen für unterschiedliche Niveaus hinsichtlich der Verbindungsqualität.

Farbe	Beschreibung
• Grün	Die Verbindungsqualität ist "Excellent" oder "Good", keine Maßnahmen erforderlich.
• Gelb	Die Verbindungsqualität ist noch "Marginal" (im Grenzbereich), keine Maßnahmen erforderlich.
• Rot	Die Verbindungsqualität ist "Poor" (schlecht), Behebungsmaßnahmen sind erforderlich. (siehe hierzu Kapitel B Problembehandlung)

Ist der SNR-Wert niedriger als erwartet, können über die Anzeigen Signal level (Signalpegel) und Noise level (Störpegel) zusätzliche Aufschlüsse gewonnen werden.

- Ein geringer Signalpegel deutet darauf hin, dass das Funksignal relativ schwach ist, d.h. die SIMATIC NET IWLCP 1515 Manager-Station befindet sich an der Grenze des Funkabdeckungsbereichs des Link Test-Partners.
- Ein hoher Störpegel deutet auf eine Störquelle im Bereich der Funkstrecke zwischen den beiden Link Test-Partnern hin.

  Durch Vergleichen der für Ihre Station und für den Link Test-Partner angezeigten Werte lässt sich die Störquelle unter Umständen lokalisieren. Sie können diese dann ausschalten und prüfen, ob sich die Performance verbessert.

5.2.2.1.2 Received Messages (empfangene Meldungen)

Anhand der Anzeige "Received Messages" können Sie die Effizienz der Funkstrecke zwischen der CP 1515 Manager-Station und dem Link Test-Partner ermitteln.

Bei der Durchführung eines Link Test tauscht die SIMATIC NET IWL CP 1515 Manager-Station mit dem Testpartner Meldungen aus. Der Testpartner bestätigt den Empfang der Meldungen durch Rücksendung entsprechender Quittungen.

Die Meldungen dienen der drahtlosen Teststation und dem Link Test-Partner zu folgenden Zwecken:

- Messung des Störabstands (Signal to Noise Ratio, SNR)
- Vergleich zwischen der Anzahl der gesendeten und der empfangenen Meldungen
  - Wird die Verbindungsqualität als "Excellent" oder "Good" eingestuft, so sollte die Anzahl verlorener (lost) Meldungen Null betragen.

— Ist die Verbindungsqualität "Marginal" (im Grenzbereich), wird die Anzahl verlorener Meldungen im Bereich von 1% bis 3% liegen.

— Liegt der Anteil der verlorenen Meldungen bei >5%, ist davon auszugehen, dass es im Netzwerk Performance-Probleme gibt.

Meistens lässt sich beobachten, dass der Anteil der verlorenen Meldungen dann ansteigt, wenn der SNR-Wert abfällt.

Die Angaben zur Anzahl der mit unterschiedlichen Übertragungsraten ("11 Mbit/s", "5.5 Mbit/s", "2 Mbit/s" und "1 Mbit/s") empfangenen Meldungen können als Indikator für die Durchsatzeffizienz im Netzwerk dienen.

Normalerweise werden verloren gegangene Meldungen (aufgrund einer Framekollision oder weil sich der Testpartner außerhalb des Funkabdeckungsbereichs befand) von den SIMATIC NET IWL -Stationen nochmals ausgesendet.

- Schlägt die Übertragung einer Meldung fehl, so sendet die drahtlose Station den "verloren gegangenen" Frame nochmals aus.
- Misslingt auch die Neuaussendung mehrmals, schaltet die Station auf eine geringere Datenrate um[1] und sendet danach die Meldung nochmals aus.

Je größer die Anzahl der mit der höchsten Übertragungsrate empfangenen Meldungen ist, desto höher ist die Durchsatzeffizienz. Ist die Anzahl der mit verringerten Übertragungsraten empfangenen Meldungen relativ hoch, kann dies auf folgendes hindeuten:

1. Die Reichweite bei der drahtlosen Datenübertragung hängt mit der Datenrate zusammen. Funkmeldungen mit einer verringerten Datenrate können über größere Entfernungen übertragen werden als Meldungen mit der höchstmöglichen Datenrate. In den meisten Netzwerk-Umgebungen lässt sich mit der Einstellung "Auto Fall-back" für die Übertragungsrate die beste Performance erlangen.

- Eine unzureichende Funkleistung, die mit dem SNR-Wert zusammenhängen kann, oder
- Engpässe im Netzwerk. Dies trifft häufig zu, wenn die SNR als "Good" eingestuft wurde.

Wird eine Vielzahl von Meldungen mit einer verringerten Datenrate (neu)ausgesendet, kann die verringerte Datenrate auf folgende Faktoren zurückzuführen sein:

- Der Link Test-Partner befindet sich an der Grenze des Funkabdeckungsbereichs der CP 1515 Manager-Station. Dies lässt sich an einem niedrigen SNR-Wert erkennen.
- Die Drahtlos-Karte eines der Testpartner unterstützt die hohen Übertragungsraten nicht.

Eine genauere Auswertung der Verbindungsqualität ist über die folgenden Schaltflächen möglich:

- **Advice** - über diese Schaltfläche erhalten Sie ausführlichere Informationen zur Verbindungsqualität sowie Hinweise zur Problembehebung und Verbesserung der Performance.
- **Freeze** - hiermit werden die dynamischen Anzeigen und die Aktualisierung der Zahlenwerte "eingefroren", um eine genauere Auswertung der angezeigen Ergebnisse zu ermöglichen.
- **Reset** - über diese Schaltfläche werden sämtliche Diagnosezähler auf Null zurückgesetzt.

  Mit Hilfe dieser Option können Sie prüfen, ob zur Verbesserung der Performance getroffene Maßnahmen erfolgreich waren, beispielsweise das Ausschalten eines Mikrowellenherdes, der als mögliche Störquelle identifiziert wurde. Nach Anklicken der Schaltfläche **Reset** wird die

Verbindungsqualität komplett neu analysiert, wobei ältere Resultate, die sich möglicherweise negativ auf die Statistik ausgewirkt haben, ignoriert werden.

- **Help** - über diese Schaltfläche können Sie allgemeine Informationen zum CP 1515 Manager Link Test aufrufen.

  Die Online-Hilfe können Sie daneben auch durch Drücken der Funktionstaste F1 an der Tastatur aufrufen.

5.2.2.2 Registerkarte Test History

Über die Registerkarte Test History können Sie die Ergebnisse des Link Tests als Liniengrafik ausgeben. Sie können bestimmen, welche Diagnoseparameter angezeigt werden sollen, und den anzuzeigenden Zeitraum festlegen. Das Zeitfenster kann dabei für die Anzeige von Daten der letzten Minute, der letzten Stunde oder der letzten 24 Stunden eingestellt werden.

Zeigt beispielsweise ein Radio Link-Modul in regelmäßigen Abständen nicht nachvollziehbare Performance-Probleme, so haben Sie mit einer Test-Historie über 24 Stunden folgende Möglichkeiten:

- Ermittlung des genauen Zeitpunkts, zu dem das Problem auftrat, im Zeitfenster
- Auswertung der Ursache des Performance-Problems ohne ständig die dynamischen Anzeigen beobachten zu müssen

5.2.2.3 Registerkarte Log Settings

Sie können die Ergebnisse der Link Test-Messungen in einer Log-Datei festhalten und anhand dieser Datei die Verbindungsqualität umfassend

auswerten. Die Messdaten können dabei automatisch in regelmäßigen Abständen oder manuell durch ein entsprechendes Kommando in die Log-Datei geschrieben werden.

Weitere Hinweise zu Log-Dateien entnehmen Sie bitte dem Abschnitt Protokollierung von Messdaten (Seite 100).

5.2.3 Fenster Site Monitor

Mit Hilfe der Option Site Monitor können Sie die Qualität der Verbindung zwischen der CP 1515 Manager-Station und sämtlichen Access Point RLMs, die innerhalb der Reichweite dieser Station liegen, abfragen.

In Roaming-Umgebungen in geschlossenen Räumen erlaubt die Funktion Site Monitor folgende Maßnahmen:

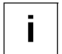
- Ermitteln des allgemeinen Funkabdeckungsgrades im SIMATIC NET IWL-Netzwerk
- Prüfung und Anpassung der Positionierung von Radio Link-Modulen, um für mobile Stationen beim Roaming einen unterbrechungsfreien Funkkontakt zu gewährleisten.

Beim Roaming mit der CP 1515 Manager-Station in einer drahtlosen Netzwerkumgebung können Bereiche identifiziert werden, wo die Funkabdeckung unzureichend ist, oder wo es zu Störungen durch andere (drahtlose) Geräte wie Türsicherungen, Mikrowellenherde oder Fotokopierer kommt.

Zum Aufrufen der Funktion Site Monitor wählen Sie im Hauptfenster des CP 1515 Manager im Menü **Advanced** die Option **Site Monitor.** Hierauf erscheint das in Abbildung 15 Fenster Site Monitor dargestellte Fenster.

5.2.3.1 Optionen im Fenster Site Monitor

- **Site Monitor** - über diese Registerkarte lässt sich die Performance des drahtlosen Netzwerks überwachen (siehe Registerkarte Site Monitor (Seite 89)).
- **Selection** - über diese Registerkarte können Sie benachbarte SIMATIC NET IWL-Netzwerke suchen und diese für die Überwachung auswählen (siehe Registerkarte Selection (Seite 93)).
- **Log Settings** - hierüber können Sie die Site Monitor Protokollierungsfunktionen aktivieren, deaktivieren oder konfigurieren (siehe Protokollierung von Messdaten (Seite 100)).
- **AP names** - hier können Sie benutzerdefinierte Access Point RLM-Namen zur einfacheren Identifizierung der Access Point RLMs im Fenster Site Monitor vergeben (siehe Registerkarte AP Names (Seite 98)).



HINWEIS:

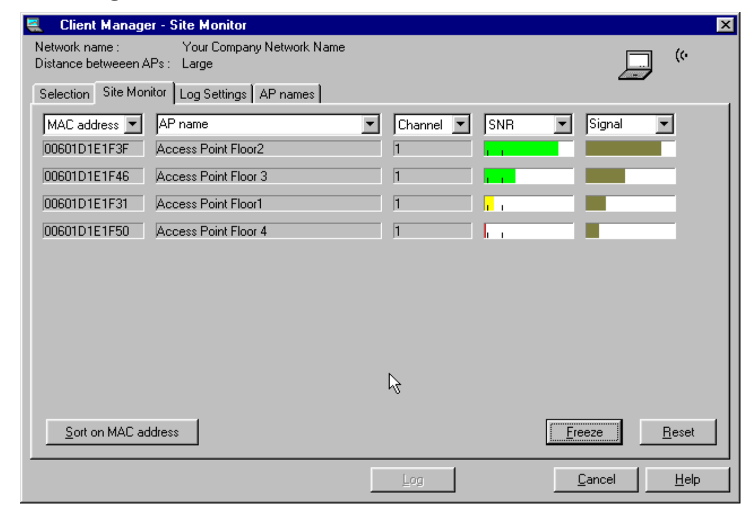
Die Option Site Monitor steht nur in Verbindung mit Access Point RLMs zur Verfügung. Wird die Option in einer Peer-to-Peer-Workgroup-Umgebung gewählt,[1] liegt im Fenster Site Monitor anstelle der Registerkarte Site Monitor die Registerkarte Selection (siehe Beschreibung in Registerkarte Selection (Seite 93)) obenauf.

5.2.3.2 Registerkarte Site Monitor

Beim Aufrufen des Fensters Site Monitor wird das in Abbildung 15 Fenster Site Monitor dargestellte Fenster angezeigt.

1. Unabhängige Netzwerke enthalten grundsätzlich keine Access Point RLMs (siehe hierzu auch Kapitel 2 Drahtlos-Konfigurationen).

Abbildung 15 Fenster Site Monitor



Im oberen Teil des Fensters Site Monitor werden folgende Informationen angezeigt:

- **Current Network (SSID)** - hier ist der Name des Netzwerks angegeben, an dem Sie momentan angeschlossen sind.
- **Distance between APs** - hier ist der durchschnittliche Abstand zwischen den RLMs im Netzwerk angegeben, an dem Sie momentan angeschlossen sind.

Diese Angaben beiben weiterhin sichtbar, wenn im Fenster Site Monitor eine andere Registerkarte aufgerufen wird.

Daneben werden im Fenster Site Monitor sämtliche Access Point RLMs angezeigt, die:

- zum selben Netz gehören, an das Sie momentan angeschlossen sind, und
- die sich innerhalb der Reichweite der CP 1515 Manager-Station befinden.

Sie können die Parameter-Einstellungen im Modus Site Monitor individuell an Ihre Bedürfnisse anpassen (siehe Beschreibung unter Anpassen der Site Monitor-Anzeige (Seite 92)). Die empfohlene Einstellung für eine normale Standortanalyse sieht folgendermaßen aus:

- **AP name** (RLM-Name) - zur Identifizierung von Geräten über den RLM-Namen

  Dieser Name wird am folgenden Ort festgelegt:

  - Im Feld **System Name** der RLM-Konfiguration (siehe SNMP-Parameter (Seite 234))
  - In einer benutzerdefinierten **Namensliste** für die Access Points (RLMs), die mit Hilfe des Tools CP 1515 Manager eingerichtet werden kann (siehe Registerkarte AP Names (Seite 98)).
- **SNR** - der Störabstand-Wert (Signal to Noise Ratio), der die Qualität der Verbindung zu den verschiedenen Access Point RLMs angibt.
- **Channel** - hier ist der Funkkanal angegeben, der von den einzelnen Access Point RLMs belegt wird.

Zum Ausführen einer Standortanalyse gehen Sie folgendermaßen vor:

1. Richten Sie die Site Monitor-Anzeige wie oben beschrieben ein.
2. Ermitteln Sie, an welchen Standplätzen im Netz eine Funkverbindung benötigt wird.
3. Gehen Sie den durch Funk abzudeckenden Bereich mit einem mobilen Computer ab.
4. Prüfen Sie beim Roaming im Netz, ob jeder Gerätestandplatz mindestens durch ein RLM abgedeckt ist, bei dem der SNR-Wert "Marginal" (Gelb), d.h. im Grenzbereich, oder besser ist.
5. (Optional) Über die Schaltfläche **Sort on** können Sie die Anzeigereihenfolge der Access Point RLMs in Abhängigkeit von den in der ersten Spalte angezeigten Daten ändern.

   Beim erstmaligen Aufrufen des Fensters Site Monitor werden die Access Point RLMs in absteigender Reihenfolge nach den jeweiligen SNR-Werten sortiert.
6. (Optional) Um die Access Point RLMs nach einem andere Kriterium zu sortieren, wählen Sie einfach in der ersten Spalte eine andere Option.

5.2.3.3 Anpassen der Site Monitor-Anzeige

Möglicherweise wollen Sie für bestimmte Zwecke noch zusätzliche Parameter einstellen, z.B.:

- Anzeige des Signalpegels (**Signal**) und des Störpegels (**Noise**) zur Ermittlung der Ursache bei einem schlechten SNR-Wert

— Ein geringer Signalpegel deutet beispielsweise auf ein schwaches Funksignal hin, d.h. das Radio Link-Modul befindet sich an der Grenze der Funkabdeckungsbereichs.

— Ein hoher Störpegel deutet auf eine Störquelle in der Nähe der Funkstrecke zwischen der CP 1515 Manager-Station und dem Access Point RLM hin.

SNR, Signalpegel und Störpegel können jeweils als dynamische Anzeigen und/oder numerische Werte in dBm angezeigt werden.

- Anzeige der **MAC-Adresse** der CP 1515 im Access Point. Diese Option ist in folgenden Fälle nützlich:

  — Sie erstellen eine Namensliste der Access Points gemäß Beschreibung in "Registerkarte AP Names (Seite 98)".

  — Im Netz gibt es RLMs, die mit mehreren IWL-Karten CP 1515 ausgestattet sind, und Sie wollen innerhalb der Access Points zwischen einzelnen Karten unterscheiden können.

5.2.3.4 Registerkarte Selection

Über die Registerkarte **Selection** können Sie ein anderes Netzwerk auswählen, etwa zu folgenden Zwecken:

- Prüfung auf evtl. vorhandene Netzwerke in der Umgebung
- Prüfung, ob von benachbarten Netzwerken Störungen auf das eigene Netzwerk ausgehen könnten

Welche Access Point RLMs beim Starten des Site Monitor-Tools angezeigt werden, wird durch die Konfiguration des Parameters Netzwerkname in der CP 1515 Manager-Station festgelegt (Option **Edit/Add Configuration**

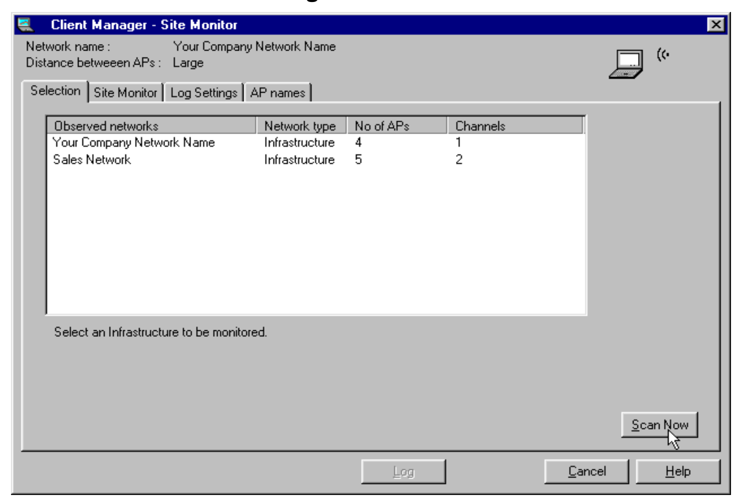
Profile im Menü **Actions** im Hauptfenster des CP 1515 Manager). Lautet die Einstellung des Netzwerknamens in der CP 1515 Manager-Station etwa:

- **Bestimmter Netzwerkname**,
  - so stellt die Station nach dem Hochlauf eine Verbindung zu dem über diesen Netzwerknamen gekennzeichneten Netz her.
  - so zeigt die Station nur die zu dem jeweiligen Netzwerk gehörenden Access Point RLMs an, die sich im Funkabdeckungsbereich der CP 1515 Manager-Station befinden.
- "**ANY**" Netzwerk,
  - so stellt die Station nach dem Hochlauf eine Verbindung zu dem ersten "offenen" Netzwerk her, das erkannt wird.
  - so zeigt die Station alle zu dem jeweiligen Netzwerk gehörenden RLMs an, die sich im Funkabdeckungsbereich der CP 1515 Manager-Station befinden.
- **Peer-to-Peer**-Workgroup:
  - es wird zwischen den einzelnen Stationen eine Workgroup mit der Einstellung Peer-to-Peer eingerichtet.

5.2.3.5 Auswahl eines anderen drahtlosen Netzwerks:

1. Klicken Sie im Fenster Site Monitor auf die Registerkarte **Selection**, um das in Abbildung 16 Auswahl eines anderen Netzwerks für die Überwachung dargestellte Fenster angezeigt zu bekommen.

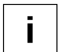
Abbildung 16 Auswahl eines anderen Netzwerks für die Überwachung



Die hierauf erscheinende Liste **Observed Networks** enthält folgende Informationen:

- Sämtliche sich im Betrieb befindliche Netzwerke innerhalb des Funkabdeckungsbereichs der CP 1515 Manager-Station
- Als Netzwerktypen kommen hierbei in Frage:
  - Infrastruktur-Netzwerk
  - Peer-to-Peer-Workgroup
- Die Anzahl der Access Point RLMs in dem oder den ermittelten Infrastruktur-Netzwerk(en)
- Die von den Access Point RLMs belegten Funkkanäle

2. (Optional) Klicken Sie auf die Schaltfläche **Scan Now**, um die Liste der ermittelten Netzwerke zu aktualisieren.
3. Klicken Sie das gewünschte Netzwerk an, um wieder zur Registerkarte Site Monitor mit den entsprechenden Diagnoseanzeigen zu gelangen.[1].



HINWEIS:

Aus Sicherheitsgründen werden Netzwerknamen und MAC-Adressen bzw. Namen von Radio Link-Modulen von benachbarten Netzwerken unter Site Monitor nicht angezeigt. Diese Werte können nur für das Infrastruktur-Netzwerk angezeigt werden, an dem Sie selbst angeschlossen sind.

Werden in der Liste **Observed Networks** keine anderen Netzwerke angezeigt, kann dies folgende Gründe haben:

1. Über die Registerkarte Selection können zwar evtl. vorhandene benachbarte unabhängige Netzwerke ermittelt werden, aber die Auswahl dieses Netzwerktyps für Site Monitor-Statistiken ist nicht möglich. Der Grund hierfür ist, dass für diese Funktion Access Point RLMs vorhanden sein müssen, was bei unabhängigen Netzwerken normalerweise nicht der Fall ist (siehe hierzu auch Drahtlos-Konfigurationen (Seite 25)).

- An der CP 1515 Manager-Station wurde ein bestimmter Netzwerkname eingerichtet.
- Bei dieser Einstellung ist die Suche nach bzw. Überwachung von anderen Netzinfrastrukturen nicht möglich. Hierfür müssen Sie den in der Station konfigurierten Netzwerknamen auf "ANY" ändern.
- In der näheren Umgebung der CP 1515 Manager-Station sind keine anderen Netzwerke in Betrieb.
- Die benachbarten Netzwerke wurden als "geschlossene" Netze eingerichet, um drahtlosen Geräten den Aufbau einer Funkverbindung zum Netz zu verwehren, die folgendermaßen konfiguriert sind:
  a. Netzwerkname "ANY" oder
  b. Zero-String SSID (gleichbedeutend zum Netzwerknamen "ANY")

  Weitere Hinweise zu "offenen" und "geschlossenen" Netzwerken entnehmen Sie bitte dem Abschnitt Sicherheit (Seite 170).

5.2.3.6 Registerkarte Log Settings

Sie können die Ergebnisse der Site Monitor-Messungen in einer Log-Datei festhalten und anhand dieser Datei die allgemeine Funkabdeckung im Netz umfassend auswerten. Die Messdaten können dabei automatisch in regelmäßigen Abständen oder manuell durch ein entsprechendes Kommando in die Log-Datei geschrieben werden.

Weitere Hinweise zu Log-Dateien entnehmen Sie bitte dem Abschnitt 5.2.4 Protokollierung von Messdaten.

5.2.3.7 Registerkarte AP Names

Über die Registerkarte **AP Names** können Sie eine benutzerdefinierte Liste von RLM-Namen erstellen, die den MAC-Adressen ihrer IWL-Karten CP 1515 zugeordnet sind.

Das Feld **AP Name** im Fenster Site Monitor zeigt den Wert des Parameters **System Name** an, der dem Access Point RLM bei der Konfiguration zugewiesen wurde[1].

Damit der Name angezeigt werden kann, muss Ihr Computer zunächst Datenverbindungen zu den entsprechenden Access Point RLMs herstellen. Das heißt, dass bis zu diesem Zeitpunkt

- der Computer noch nicht den Standort gewechselt hat
- die Registerkarte **AP Names** noch nicht aufgerufen wurde.

Beim Ausführen des Tools CP 1515 Manager im Modus Site Monitor können Sie über die Registerkarte **AP Names** jeder Access Point RLM-MAC-Adresse, auf die Sie stoßen, kurzerhand einen RLM-Namen zuweisen.

Sollten Sie auf Access Point RLMs stoßen, die als "unknown" (unbekannt) gekennzeichnet sind, gehen Sie folgendermaßen vor:

1. Rufen Sie die Registerkarte **AP Names** auf.
2. Geben Sie eine MAC-Adresse ein oder doppelklicken Sie auf eine der MAC-Adressen in der Liste.
3. Geben Sie im Feld **Access Point Name** einen Namen ein, über den sich das Radio Link-Modul leicht identifizieren lässt.

1. Um dem Access Point RLM einen Systemnamen zuweisen zu können, müssen Sie den betreffenden Namen zunächst mit dem Programm RLM Manager im Fenster “SNMP-Parameter” (siehe Abbildung 41 SNMP-Parameter einrichten) eingeben.

4. Klicken Sie als Nächstes auf die Schaltfläche **Add to Table**, um den Namen der ausgewählten MAC-Adresse zuzuordnen.
5. Wiederholen Sie die Schritte 2 bis 4 für sämtliche anderen MAC-Adresssen.
6. Rufen Sie nach Abschluss Ihrer Eingaben wieder die Registerkarte **Site Monitor** auf, um mit der Standortanalyse fortzufahren.

Beim Abgehen der drahtlosen Netzwerkumgebung werden Sie unter Umständen neue MAC-Adressen auftauchen sehen, wenn Sie sich anderen Access Point RLMs nähern. Ist dies der Fall, wiederholen Sie die oben beschriebenen Schritte, um die Access Point (RLM)**-Namenstabelle** zu vervollständigen.

Die Radio Link Module-Namen, die Sie den vorgefundenen MAC-Adressen zuordnen, werden in einer ASCII-Datei gespeichert.

Diese Datei können Sie gemeinsam mit anderen LAN-Administratoren nutzen, die mit Hilfe des Tools CP 1515 Manager die das drahtlose Netzwerk auf seine Performance prüfen. Die Datei ("APlist.text") wird im folgenden Verzeichnis abgelegt:

C:\Programme\Siemens I-Gate\Clientmanager

- Mit einem ASCII-Editor, wie z.B. dem Editor von MS-Windows, können Sie die Namen nachträglich bearbeiten.

5.2.4 Protokollierung von Messdaten

Die Funktionen Link Test und Site Monitor erlauben beide das Protokollieren von Messergebnissen. Die Protokollierung kann dabei manuell oder automatisch in regelmäßigen Abständen angestoßen werden.

Der CP 1515 Manager speichert die Daten in einer CSV (Comma Separated Value)-Datei ab, von wo aus sie für weitere Auswertungen in Standard-Tabellenkalkulations- oder Datenbank-Anwendungen importiert werden können.

Mittels Vergleichen der Messdaten mit älteren Messungen können Sie die Performance des Drahtlos-LANs über einen längeren Zeitraum verfolgen und beispielsweise die Auswirkungen von Umstellungen im Netzwerk untersuchen.

Die Fenster Link Test und Site Monitor verfügen über beinahe identische Protokollierungs-Parameter. Der einzige Unterschied besteht darin, dass beim Link Test eine fortlaufende Protokollierung unterstützt wird, bei Site Monitor jedoch nicht.

5.2.4.1 Manuelle Protokollierung von Daten

Mit Hilfe der Funktion "Manual data logging" können Sie eine Momentaufnahme der Messdaten machen, beispielsweise, wenn Sie gerade mit der Funktion Site Monitor eine Standortanalyse durchführen oder wenn Sie eine bestimmte Störquelle untersuchen.

Im Modus Manuell können Sie ergänzend die Option **Add comments to log** aktivieren, die es Ihnen erlaubt, die protokollierten Daten mit eigenen Anmerkungen (z.B. zum Standort oder Hergang) zu versehen. Ist diese

Option aktiviert, so erscheint immer wenn Sie die Schaltfläche **Log Once** betätigen ein entsprechendes Dialogfeld.

Die Option "Manual data logging" bietet sich insbesondere für Site Monitor-Prüfungen mit CP 1515 Manager-Stationen im Roaming-Modus an.

5.2.4.2 Automatische Protokollierung von Daten

Mit Hilfe der Funktion "Automatic data logging" können Sie Daten zur Netz-Performance automatisch in vorgegebenen Abständen protokollieren. Dies kann von Nutzen sein, wenn Sie wiederkehrende Vorgänge oder Wertschwankungen über einen längeren Zeitraum erfassen wollen.

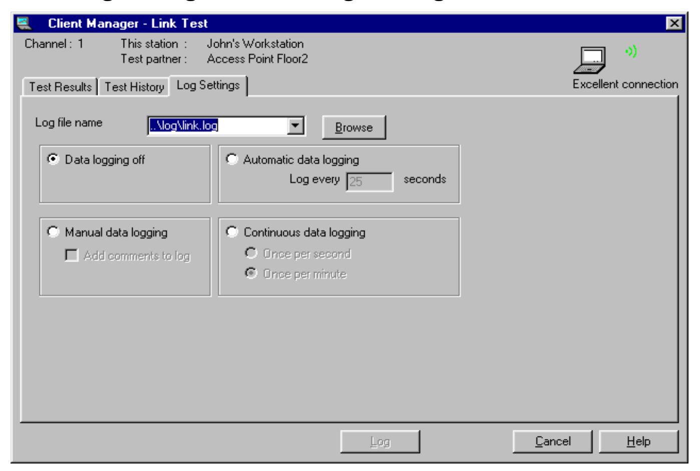
Bei Auswahl des Modus Automatisch müssen Sie für das Messintervall einen bestimmten Wert in Sekunden eingeben.

Die Funktion "Automatic data logging" bietet sich dann an, wenn mit der CP 1515 Manager-Station ein Link Test an einem bestimmten Standort vorgenommen wird.

5.2.4.3 Einstellen der -Optionen

1. Klicken Sie im Fenster Link Test oder Site Monitor auf die Registerkarte **Log Settings**, um das in Abbildung 17 Registerkarte Log Settings abgebildete Fenster aufzurufen.

Abbildung 17 Registerkarte Log Settings



2. Geben Sie im Feld **Log file name** einen Namen für die Log-Datei ein. Optionen:
   - Eingabe eines neuen Dateinamens - es wird eine neue Datei angelegt.
   - Beibehaltung des vorhandenen Dateinamens - neue Daten werden am Ende der Datei angehängt.
   - Verwendung des voreingestellten Namens - neue Daten werden am Ende der Datei angehängt.

3. Wählen Sie den Protokollierungsmodus:
   - **Data logging off** - es erfolgt keine Protokollierung.
   - **Manual data logging** - Aufzeichnung der Link-Messung wird manuell angestoßen. Wenn Sie das Kontrollkästchen "Add comments" aktivieren, können Sie bei der Protokollierung von Daten jeweils eigene Anmerkungen hinzufügen.
   - **Automatic data logging** - Daten werden automatisch aufgezeichnet. Hier muss ein Intervall eingegeben werden, in welchem die Messungen angestoßen werden.
   - **Continuous data logging** (nur beim Fenster Link Test) - Daten werden automatisch in folgenden Intervallen aufgezeichnet:
     a. **Once per second** oder
     b. **Once per minute**

Die Messdaten werden bei allen Modi in der im Feld **Log file name** eingetragenen Datei gespeichert. Neu zu speichernde Daten werden dabei jeweils ans Ende der bestehenden Datei angefügt. Sollen die Daten in einer neuen Datei abgelegt werden, geben Sie in dem betreffenden Feld einen neuen Dateinamen ein.

5.2.4.4 Starten/Stoppen der Protokollierungs-Funktion

Je nach der von Ihnen gewählten Option erscheint als Aufschrift auf der Logging-Schaltfläche entweder **Log Once** (manueller Start) oder **Start Log** (automatischer Start).

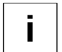
- Bei manueller Protokollierung klicken Sie auf die Schaltfläche "Log Once", wenn Sie die Aufzeichnung starten wollen. Die Aufzeichnung wird automatisch gestoppt, nachdem die Daten in die Log-Datei geschrieben wurden.
- Für eine automatische Protokollierung klicken Sie auf die Schaltfläche **Start Log**. Beenden können Sie die Aufzeichnung durch Anklicken der Schaltfläche **Stop Log**.

5.2.5 Diagnose Card

Wenn der Verdacht besteht, dass der CP 1515 nicht ordnungsgemäß funktioniert, können Sie mit der Option **Diagnostics** im Menü **Advanced** im Hauptfenster des CP 1515 Manager die Hardware und Software der Karte auf ihre Funktion überprüfen.

Im Fenster Diagnose Card können Sie Informationen zu Software, Firmware und Konfiguration abrufen sowie Verbindungsstatistiken ansehen.

Um die Funktion des CP 1515 zu prüfen, klicken Sie in der Registerkarte **Card Check** auf die Schaltfläche **Test Card Now**.



HINWEIS:

Durch diesen Test wird der CP 1515 in seinem normalen Betrieb unterbrochen, wodurch es zu einem vorübergehenden Abbruch der Verbindung zum Netz kommen kann.

Hat der CP 1515 sämtliche Tests bestanden, erscheint als Prüfzustand in sämtlichen Feldern "OK" und das Feld Error Code bleibt leer. Wurde ein

Fehler gefunden, erhalten Sie über die Schaltfläche **Advice** Hinweise zur Fehlerbehandlung.

5.2.6 Problembehandlung im Modus Site Monitor

Werden bei der Funktion Site Monitor nicht alle erwarteten Access Point RLMs angezeigt, kann dies folgende Gründe haben:

- Die CP 1515 Manager-Station befindet sich außerhalb des Funkabdeckungsbereichs der Access Point RLMs, die geprüft werden sollen. In diesem Fall beträgt der Wert für den Signalpegel und die SNR normalerweise ’0’ (Null).
- Eine Fehlkonfiguration der CP 1515 Manager-Station, z.B.:
  - Der in der CP 1515 Manager-Station eingetragene Netzwerkname stimmt nicht mit dem Namen des Netzes überein, das überwacht werden soll.
  - In der CP 1515 Manager-Station ist als Netzwerkname "ANY" eingetragen. Beim Hochlauf der Station stellte diese eine Verbindung zu einem RLM eines benachbarten Netzwerkes her, weil dieses RLM den besten SNR-Wert hat.
- Das Netzwerk, das geprüft werden soll, wurde für drahtlose IEEE 802.11-kompatible Geräte gesperrt, die mittels folgender Optionen versuchen, eine Funkverbindung herzustellen:
  - Netzwerkname "ANY" oder
  - Zero-String SSID (gleichbedeutend zum Netzwerknamen "ANY")

Ist in der CP 1515 Manager-Station als Netzwerkname "ANY" eingetragen, können Sie über die Registerkarte **Selection** andere Netzwerke anzeigen (siehe Abschnitt Registerkarte Selection (Seite 93)).

Weitere Hinweise zu "offenen" und "geschlossenen" Netzwerken entnehmen Sie bitte dem Abschnitt Sicherheit (Seite 170).

5.3 Einsatz des RLM Manager

Mit Hilfe des RLM Manager können Sie:

- Eine Reihe von Standard-SNMP-Variablen anzeigen und hierüber die allgemeine Performance des LAN-Netzwerks überwachen (siehe auch Registerkarte Remote Statistics (Seite 118))
- Die Ergebnisse von Remote Link Test-Messungen (siehe Fenster Remote Link Test (Seite 112)) zwischen einem (entfernten) Access Point RLM und einer an dem ausgewählten Access Point RLM angeschlossenen drahtlosen Station anzeigen

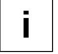
Der RLM Manager ist für die Überwachung des Netzwerks von einem zentralen Standort (z.B. der LAN-Administratorstation) ausgelegt und erlaubt die Prüfung der Funkleistung in Bereichen, die nicht ohne Weiteres zugänglich sind (z.B. drahtlose Netzwerke an entfernten Standorten).

5.3.1 Überwachungs-Optionen

Das Programm RLM Manager bietet eine Reihe von Diagnosefunktionen, wovon die folgenden drei für den Standardbenutzer am relevantesten sind:

- Systemdaten (siehe Systemdaten (Seite 110))
- Remote Link Test (siehe Fenster Remote Link Test (Seite 112))
- Remote-Statistik (siehe Registerkarte Remote Statistics (Seite 118))

Bei allen anderen Diagnosefunktionen handelt es sich um Standard-SNMP-Parameter, die im vorliegenden Handbuch nicht behandelt werden, jedoch in der Online-Hilfe des Programms RLM Manager dokumentiert sind.



HINWEIS:

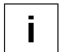
Sämtliche Diagnosefunktionen sind in der Online-Hilfe des RLM Manager beschrieben. Diese können Sie über die Funktionstaste F1 oder durch Anklicken der Schaltfläche **Help** im Fenster RLM Manager aufrufen.

5.3.2 Verbindungen zu Access Point RLMs

Zum Überwachen eines Radio Link-Moduls müssen Sie zunächst eine Verbindung zum Ziel-Radio Link Module herstellen.

1. Starten Sie das Programm RLM Manager.
2. Wählen Sie das Ziel-RLM aus der vorhandenen Liste aus oder geben Sie die IP-Adresse des Access Point RLM ein, das überwacht werden soll.

   Alternativ dazu können Sie im Menü die Option **Refresh** Radio Link Module RLM List **aufrufen und damit alle im Subnetz vorhandenen** Access Point RLMs **anzeigen.**



HINWEIS:

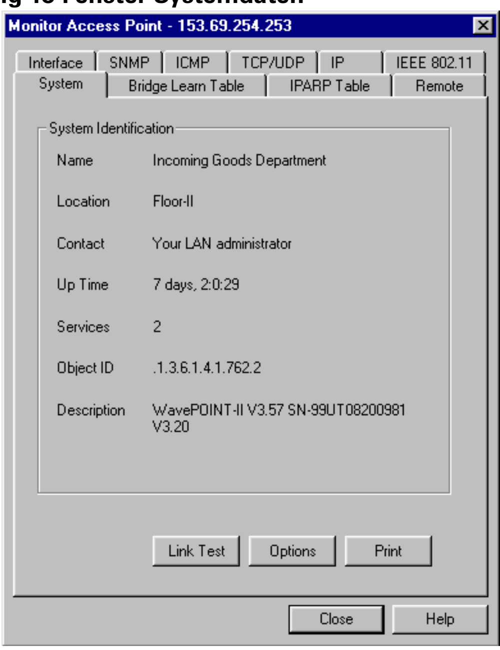
In der Liste werden nur die Access Point RLMs angezeigt, die sich im selben Subnetz wie die Manager-Station befinden. Soll eine Verbindungsstrecke außerhalb des Subnetzes untersucht werden, geben Sie im Feld **Enter the IP address of a specific Access Point** die IP-Adresse des jeweiligen RLM ein.

3. Klicken Sie auf **Monitor** , um eine Verbindung zum Ziel-Radio Link Module herzustellen.

4. Das RLM Manager-Fenster erscheint im Monitor-Modus wie in Abbildung 18 Fenster Systemdaten dargestellt.

   Sie können nun das Netzwerk überwachen.

Abbildung 18 Fenster Systemdaten



5.3.3 Systemdaten

Das Fenster System liefert keine Online-Statistiken, sondern dient in erster Linie zur Ermittlung des Ausgabestands der im Access Point RLM geladenen eingebetteten Software.

Um die Systemdaten für ein RLM abfragen zu können, müssen Sie zunächst eine Verbindung zum Ziel-RLM herstellen (siehe Verbindungen zu Access Point RLMs (Seite 108)).

Zum Ansehen der Systemdaten wählen Sie die Registerkarte **System**.

- In den Feldern **Name, Location** und **Contact** erscheinen die Werte, die bei der Konfigurierung des Acces Points RLM in den entsprechenden Feldern der Registerkarte **SNMP** eingetragen wurden.

  Zu Hinweisen, wie Sie die entsprechenden Namen ändern können, schlagen Sie bitte im Abschnitt SNMP-Parameter (Seite 234) nach.
- Im Feld **Up Time** wird das Zeitintervall seit dem letzten Rücksetzen des Radio Link-Moduls angezeigt. Ist dieser Wert niedriger als erwartet, kann das daran liegen, dass das RLM manuell zurückgesetzt oder automatisch neu gestartet wurde.
- Die in den Feldern **Services** und **Object ID** angezeigten Informationen sind für den Endbenutzer nicht relevant. Diese Werte sowie der Inhalt des Feldes **Description** werden nur für Problemmeldungen an den Technischen Support benötigt.

  Durch die Weitergabe dieser Angaben an den Support-Mitarbeiter helfen Sie diesem bei der Ermittlung der Fehlerursache.

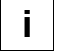
  Zum Melden von Problem können Sie wie folgt vorgehen:

  - Drucken Sie die jeweiligen Informationen über die Schaltfläche **Print** aus und senden Sie diese zusammen mit der Problemmeldung per Fax an den Technischen Support, oder
  - Drücken Sie gleichzeitig die Tasten ALT und Druck S- um den Inhalt des Fensters in die Zwischenablage zu kopieren und fügen Sie die Bildschirmabbildung in die E-Mail ein, mit der Sie dem Technischen Support das Problem melden.

- Das Feld **Description** ist das wichtigste Feld im Fenster System. Anhand dieses Feldes können Sie rasch ermitteln, ob das Access Point RLM mit der aktuellen eingebetteten Software läuft oder ob für die Unterstützung sämtlicher benötigter SIMATIC NET IWL-Funktionen ein Upgrade erforderlich ist.

  Das Feld **Description** enthält mehrere Zeichenfolgen, die folgende Informationen liefern:

  - Art der Netzwerkkomponente
  - Art und Version der im Access Point RLM geladenen eingebetteten Software. Der Wert lautet dabei etwa:
    - **VX.xx** zur Identifizierung von Software, die lediglich Access Point-Funktionen unterstützt
  - Die Zeichenfolge mit dem Format **SN-xxUTxxxxxxxx** bezeichnet die Seriennummer des RLM
  - Die abschließende Zeichenfolge mit dem Format **VX.xx** gibt die Version der Hardware in der "Prozessor-Baugruppe" des RLM an.



HINWEIS:

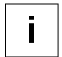
Updates zur eingebetteten Software für die Access Point RLMs werden normalerweise über die MOBIC-Website (**http://www.siemens.com/mobic**) und bei neuen Freigaben auf Software-CDs herausgegeben.

Es wird empfohlen, in festen Abständen die MOBIC-Website aufzurufen, damit Sie über eventuell verfügbare neuere Software-Versionen für die Access Point RLMs auf dem Laufenden sind.

5.3.4 Fenster Remote Link Test

Mit Hilfe der Remote Link Test-Funktion des RLM Manager können Sie die Funkstrecke zwischen einem Access Point RLM (der "Initiator-Station") und einer an dem ausgewählten RLM angeschlossenen Station prüfen.

Bei letzterer kann es sich um eine drahtlose Station handeln.



HINWEIS:

Der Remote Link Test funktioniert nur in Verbindung mit SIMATIC NET Radio Link Modulen RLM.

Die Bedienoberfläche der Remote Link Test-Funktion des RLM Manager unterscheidet sich nur geringfügig von der des Link Test beim CP 1515 Manager.

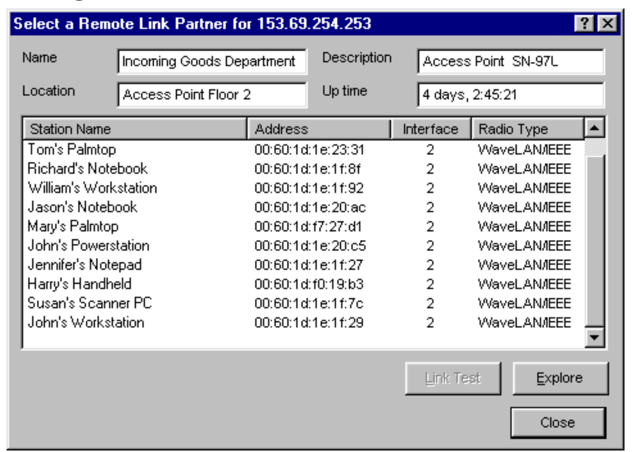
5.3.4.1 Starten des Remote Link Tests

Um die Remote-Statistik für ein Radio Link-Modul abfragen zu können, müssen Sie zunächst eine Verbindung zum Ziel-RLM herstellen (siehe Verbindungen zu Access Point RLMs (Seite 108)).

1. Wählen Sie die Registerkarte **System** und klicken Sie auf die Schaltfläche **Link Test**, um das in Abbildung 19 Fenster Select a Link Test Partner abgebildete Fenster aufzurufen.

   Die Felder im oberen Bereich des Fensters beziehen sich auf die "Initiator-Station", die beim Herstellen der Verbindung zum Access Point RLM ausgewählt wurde.

Abbildung 19 Fenster Select a Link Test Partner



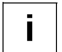
Im mittleren Bereich des Fensters "Select Remote Link Partner for ..." werden sämtliche drahtlosen Geräte aufgelistet, die an der "Initiator-Station" angeschlossen sind. Im Einzelnen werden folgende Informationen angezeigt:

- **Station Name** und **Address**. Die aufgeführten drahtlosen Geräte werden jeweils durch einen Namen und eine MAC-Adresse identifiziert.

  Der Inhalt der Liste kann sich ändern, wenn mobile Stationen den Funkabdeckungsbereich des ausgewählten RLM betreten oder verlassen.

- In der Spalte **Interface** ist jeweils der Steckplatz des Radio Link-Moduls angegeben, an dem die PC Card CP 1515 angesteckt ist.
  - 2 = Steckplatz A
  - 3 = Steckplatz B
- In der Spalte **Radio Type** ist die Art der PC-Karte (im entsprechenden Steckplatz) angegeben:
  - IEEE 802.11 für PC Cards (CP 1515)

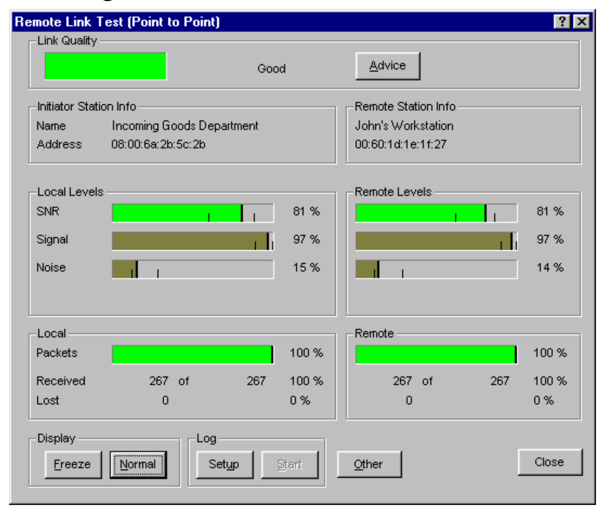
2. (Optional) Zum Aktualisieren der Liste klicken Sie auf die Schaltfläche **Refresh**.
3. Wählen Sie eine Station aus der Liste aus und klicken Sie auf die Schaltfläche **Link Test**, um das in Abbildung 20 Fenster Remote Link Test abgebildete Fenster Remote Link Test aufzurufen.



HINWEIS:

Der Aufbau des Fensters Remote Link Test kann abhängig von dem für die drahtlose Netzwerk-Schnittstelle ausgewählten "Radio Type" variieren. Das in Abbildung 20 Fenster Remote Link Test dargestellte Fenster entspricht dem für eine drahtlose Netzwerk-Schnittstelle.

Abbildung 20 Fenster Remote Link Test



5.3.4.2 Wichtige Indikatoren

Die Anzeige SNR (Signal to Noise Ratio, Störabstand) gibt die Qualität der Funkstrecke zwischen der Initiator-Station (d.h. dem Radio Link-Modul) und der Partnerstation beim Remote Link Test an.

Die Farbe der SNR-Anzeige und die Anzeigen Link Quality und Remote Levels stehen jeweils für folgende Abstufungen hinsichtlich der Verbindungsqualität:

Farbe	Beschreibung
• Grün	Die Verbindungsqualität ist "Good", keine Maßnahmen erforderlich.
• Gelb	Die Verbindungsqualität ist noch "Marginal" (im Grenzbereich), keine Maßnahmen erforderlich.
• Rot	Die Verbindungsqualität ist "Poor" (schlecht), Behebungsmaßnahmen sind erforderlich. (siehe Problembehandlung (Seite 266))
• Keine	Keine Verbindung

Ist der SNR-Wert niedriger als erwartet, können über die Anzeigen Signal (Signalpegel) und Noise (Störpegel) zusätzliche Aufschlüsse gewonnen werden.

Um die Anzeigen Signal Level und Noise Level aufzurufen, klicken Sie auf die Schaltfläche **Details**.

- Ein geringer Signalpegel deutet darauf hin, dass das Funksignal relativ schwach ist, d.h. die Partnerstation des Access Point RLM nähert sich der Grenze des Funkabdeckungsbereichs.
- Ein hoher Störpegel deutet auf eine Störquelle im Bereich der Funkstrecke zwischen dem RLM und den Link Test-Partnerstationen hin.

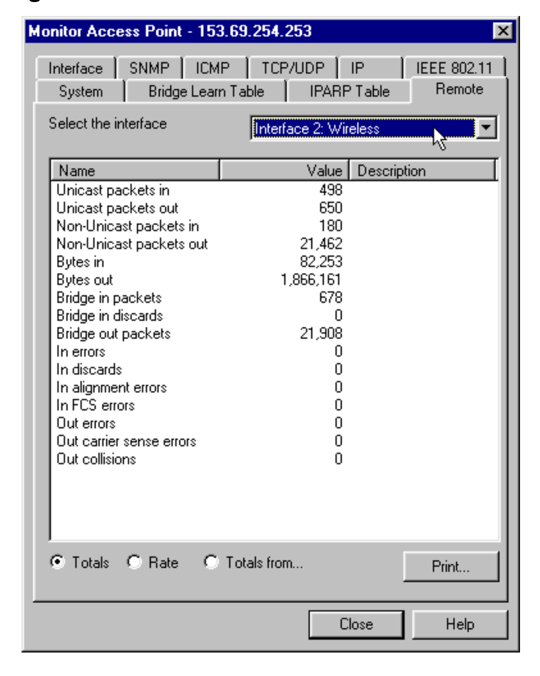
Durch Vergleichen der für das Access Point RLM und dessen Link Test-Partner angezeigten Werte lässt sich die Störquelle unter Umständen lokalisieren. Sie können diese dann ausschalten und prüfen, ob sich die Performance verbessert.

Weitere Hinweise zum Fenster Remote Link Test entnehmen Sie bitte der RLM Manager Online-Hilfe, die Sie über die Schaltfläche **Help** oder durch Betätigen der Funktionstaste [F1] aufrufen können.

5.3.5 Registerkarte Remote Statistics

Mit Hilfe der Option Remote Statistics können Sie für jede RLM-Schnittstelle (Ethernet und drahtlos) eine Reihe von SNMP-Variablen prüfen.

Abbildung 21 Remote-Statistikdaten



5.3.5.1 Starten der Remote-Statistik

Um die Remote-Statistik für ein Radio Link-Modul abfragen zu können, müssen Sie zunächst eine Verbindung zum Ziel-RLM herstellen (siehe Verbindungen zu Access Point RLMs (Seite 108)).

1. Um die Remote-Statistik anzuzeigen, wählen Sie im -Fenster im Monitor-Modus die Registerkarte RLM ManagerRemote (siehe Abbildung 21 Remote-Statistikdaten).

Für jede Schnittstelle des ausgewählten Access Point RLM lässt sich durch Auswahl der jeweiligen Schnittstelle im Pull-Down-Menü **Select the interface** die Performance anzeigen.

5.3.5.2 Wichtige Indikatoren

Unter der Registerkarte **Remote** im RLM Manager werden zahlreiche Variablen angezeigt, die Informationen zur Performance des ausgewählten RLM liefern.

Der für die Überwachung wichtigste Indikator ist das **Verhältnis zwischen Errors und Bridge Packets**. Hier gibt es drei Verhältniswerte, die von besonderer Bedeutung für die Diagnose sind:

- In errors / Bridge in packets
- Out errors / Bridge out packets
- Out collisions / Bridge out packets

Die nachfolgende Tabelle liefert entsprechende Diagnoseinformationen zu den jeweiligen Verhältniswerten.

Table 1 Verhältnis Errors/Bridge Packets

Verhältnis Errors/Bridge Packets	Bedeutung	
0,1% oder weniger	Zustand:	Die Performance ist gut
	Auswirkung:	Keine
	Erforderliche Maßnahmen:	Keine
0,1% bis 1%	Zustand:	Die Performance ist zufriedenstellend
	Auswirkung:	Die Performance des Netzwerks ist soweit in Ordnung, jedoch nicht so gut, wie zu erwarten wäre
	Erforderliche Maßnahmen:	Siehe Optimierung der Leistungsfähigkeit (Seite 126) zu Hinweisen, wie Sie die Ursache des Problems lokalisieren und die Performance des Netzwerks verbessern können
1% oder mehr	Zustand:	Die Performance ist unzureichend
	Auswirkung:	Das Performance-Problem kann von der Verkabelung oder den Anschlüssen im Netzwerk herrühren
	Erforderliche Maßnahmen:	Siehe Optimierung der Leistungsfähigkeit (Seite 126) zu Maßnahmen zur Problembehebung

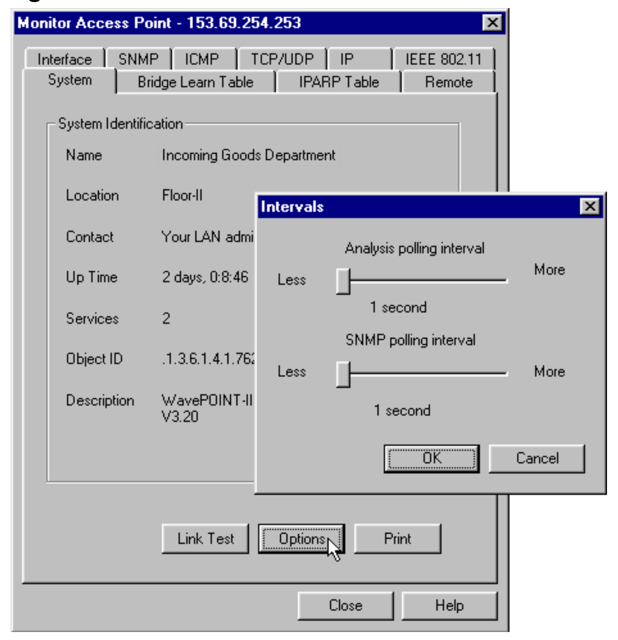
2% oder mehr	Zustand:	Die Performance ist völlig unzureichend
	Auswirkung:	Im Betriebssystem des Netzwerks kommt es vermutlich zu schwerwiegenden Performance-Problemen
	Erforderliche Maßnahmen:	Siehe Optimierung der Leistungsfähigkeit (Seite 126) zu detaillierten Angaben zur Problembehandlung. Unter Umständen sollte ein externer Fachmann zu Rate gezogen werden.

5.3.6 System Intervals

Um die System-Intervall-Parameter für die Überwachung des RLM anzuzeigen, müssen Sie zunächst eine Verbindung zum Ziel-Access Point RLM herstellen (siehe Verbindungen zu Access Point RLMs (Seite 108)).

Wählen Sie die Registerkarte **System** und klicken Sie auf die Schaltfläche **Options**, um das in Abbildung 22 Fenster Intervals abgebildete Fenster aufzurufen.

Abbildung 22 Fenster Intervals



Im Fenster Intervals kann der Zeitabstand für die Überwachung über zwei Intervall-Parameter eingestellt werden.

- Analysis polling interval (für den Remote Link Test)
- SNMP polling interval (für SNMP-Statistiken)

5.3.6.1 Einstellen des Analysis Polling Interval

Je nach Art der Verbindung können Sie die Aktualisierungsrate für die Remote Link Test-Ausgabe, auch Analysis Polling Interval (Auswertungs-Abfrageintervall) genannt, flexibel anpassen.

Beim Remote Link Test werden fortlaufend Messergebnisse erfasst, wobei das ausgewählte Radio Link-Modul (Initiator-Station) die Ergebnisse in festen Abständen zwischen 1 und 15 Sekunden zur LAN-Administratorstation überträgt.

- Wählen Sie ein kurzes Intervall (z.B. 1 Sekunde) für die Online-Überwachung, z.B. für Problembehandlungs-Maßnahmen oder wenn beim Zugang über das Netzwerk die volle Bandbreite zur Verfügung steht.
- Wählen Sie ein längeres Intervall (z.B. 15 Sekunden), wenn der Remote Link Test lediglich routinemäßig erfolgt, oder wenn der Zugriff auf das Netzwerk über eine langsame Verbindung (z.B. eine Modem-Wählverbindung) erfolgt.

5.3.6.2 Einstellen des SNMP Polling Interval

Die auf der Registerkarte **Remote** angezeigten Daten werden in regelmäßigen Abständen aktualisiert, die zwischen 1 Sekunde und 5 Minuten liegen können. Durch Ändern des Wertes SNMP polling interval kann die Aktualisierungsrate flexibel angepasst werden.

- Wählen Sie ein kurzes Intervall (z.B. 1 Sekunde), wenn die Remote-Statistik online verfolgt werden soll, z.B. für Problembehandlungs-Maßnahmen und/oder wenn beim Zugang auf das RLM über das Netzwerk die volle Bandbreite zur Verfügung steht.
- Wählen Sie ein langes Intervall (z.B. 5 Minute), wenn die Remote-Statistik lediglich routinemäßig abgefragt wird und wenn der Zugriff auf das Netzwerk des ausgewählten Radio Link Module über eine langsame Verbindung (z.B. eine Modem-Wählverbindung) erfolgt.

6 Optimierung der Leistungsfähigkeit

6.1 Einführung

Die Leistungsfähigkeit Ihres LAN hängt normalerweise von einer komplexen Kombination unterschiedlicher Faktoren ab. In diesem Abschnitt finden Sie Tips und Anregungen, die Ihnen dabei helfen werden,

- zu entscheiden, ob eine Optimierung tatsächlich erforderlich ist, und
- Ihr SIMATIC NET IWL anzupassen, um die Leistung zu optimieren.

Eine Optimierung der Netzwerkleistung ist in folgenden Fällen sinnvoll:

- um ein potentielles Problem zu behandeln,
- wenn die Leistungsfähigkeit des LAN nicht Ihren Erwartungen entspricht, oder
- wenn regelmäßige Routinechecks auf eine Verschlechterung der Leistung schließen lassen.

In diesem Kapitel werden unterschiedliche Lösungsmöglichkeiten für häufig auftretende Probleme dargestellt.



ACHTUNG:
Bevor Sie die Konfiguration(en) ändern, sollten Sie separate Sicherheitskopien der Konfigurationsdaten für jedes Access Point RLM erstellen. Auf diese Weise können Sie die ursprüngliche Konfiguration wiederherstellen, falls Ihre Maßnahmen zur Lösung des Problems erfolglos waren.

6.2 Beseitigung von unnötigem Verkehr

Alle Daten, die in Ihrem Netzwerk übertragen werden, lassen sich prinzipiell in zwei Datentypen unterteilen:

- Echte Daten: hierbei handelt es sich um Daten, die zwischen Netzstationen ausgetauscht werden, z.B. Datei-Transfer oder E-Mail. “Echte Daten” werden in der Regel als “Netzlast” bezeichnet und schliessen auch Telegramme ein, die aufgrund von Kollisionen, fehlerhaften Kabelverbindungen bzw. unzureichenden Funkverbindungen zwei- oder mehrmals übertragen werden.

  Im Monitormodus werden auf der Registerkarte Remote des RLM Manager die "echten Daten" als Unicast-Pakete angezeigt.

- Bei den Netzwerk-Verwaltungsdaten handelt es sich um Daten, die zwischen den Netzdiensten ausgetauscht werden, um den Datenfluss zu steuern. Verwaltungsdaten werden in der Regel als “Verkehrslast” bezeichnet und beinhalten Protokoll- und Broadcast-Telegrammen und/ oder Fehlermeldungen aufgrund inkompatibler Konfigurationen.

  Im Monitormodus werden die "Netzwerk-Verwaltungsdaten" in der Registerkarte Remote des RLM Manager als Non-Unicast-Pakete angezeigt.

Das Verhältnis zwischen Netzwerk-Verwaltungsdaten und “echten Daten” variiert von einem Netzwerk-Dienst zum anderen. Wenn der Anteil an Netzwerk-Verwaltungsdaten höher als aktuell benötigt ist, kann es zu einer Beeinträchtigung der Leistungsfähigkeit Ihres drahtlosen LAN kommen. Dies ist darauf zurückzuführen, dass Ihre “echten Daten” die verfügbare Bandbreite mit den Netzwerk-Restkapazitäten teilen müssen.

Durch die Beseitigung von unnötigem Verkehr kann die Leistungsfähigkeit Ihres IWL-Netzwerks deutlich verbessert werden. Mit dem RLM Manager können Sie eine oder mehrere der folgenden Optionen wählen:

- Protokollfilterung (Seite 129): Protokolle filtern, die für drahtlose Stationen nicht relevant sind.
- Optimierung von drahtgebundenen Verbindungen (Seite 133): Unnötige Fehlermeldungen zu fehlerhaften Verbindungen beseitigen.
- Optimierung von drahtlosen Verbindungen (Seite 138): Die erneute Übertragung verlorener oder kollidierter Telegramme vermeiden.
- Optimierung durch Vorschalten eines Switches (z.B. ESM TP80) vor das RLM Ethernet Interface. Der Switch leitet nur den Telegrammverkehr zum RLM, der für Teilnehmer in der Funkzelle bestimmt ist.

6.2.1 Protokollfilterung

Manche Netzwerkprotokolle senden eine große Anzahl an Broadcast-Telegrammen an alle Stationen. In vielen Fällen werden diese Protokolle aber von Ihren drahtlosen Stationen gar nicht benötigt. Hier kann mittels Protokollfilterung die Übertragung unnötiger Daten vermieden werden und zusätzliche Bandbreite für die Übertragung “echter Daten” bereitgestellt werden.

6.2.2 Benötigt Ihr Netzwerk Protokollfilterung?

Um festzustellen, ob das Protokoll-Broadcasting die Leistungsfähigkeit eines drahtlosen Netzwerks beeinträchtigt, können Sie die Registerkarte Registerkarte Remote Statistics (Seite 118) verwenden.

1. Starten Sie den RLM Manager, wählen Sie das Access Point RLM und klicken Sie auf die Schaltfläche **Monitor**.
2. Wählen Sie **Remote Statistics** im Menü **Monitor**.
3. Wählen Sie die Registerkarte **Remote**, um die Schnittstellen-Statistik anzuzeigen.
4. Vergleichen Sie die Anzahl der **Out collisions** mit der Anzahl der **Bridge out packets**.
   - Ist der Anteil der “Out collisions” in den “Bridge out packets” geringer als 1%, ist die Leistungsfähigkeit des drahtlosen Mediums gewährleistet. Eine Protokollfilterung ist nicht erforderlich, kann jedoch in Betracht gezogen werden.
   - Wenn hingegen der Anteil der "Out collisions" in den "Bridge out packets" über 1% liegt, deutet dies auf einen regen Datenverkehr im drahtlosen Medium hin.

     Ist die Anzahl der Benutzer sowie das Verkehrsaufkommen im Netzwerk verhältnismäßig niedrig, kann es sinnvoll sein, zu prüfen, ob sich die Leistungsfähigkeit Ihres Netzwerks mittels Protokollfilterung erhöhen lässt.
5. Vergleichen Sie die Anzahl der **Unicast packets out** mit der Anzahl der **Non-Unicast packets out**.

- Ist die Zahl der “Non-Unicast packets out” im Vergleich zu den “Unicast packets out” relativ hoch, kann dies auf ein hohes Verkehrsaufkommen in Ihrem Netzwerk hindeuten.

  Dies bedeutet jedoch nicht notwendigerweise, dass die Verkehrslast auf die Protokolle zurückzuführen ist - allerdings kann es auch hier sinnvoll sein zu prüfen, ob die Leistungsfähigkeit Ihres Netzwerks mittels Protokollfilterung verbessert werden kann.



ACHTUNG:
Unter Umständen ist eine umfassende Netzwerkerfahrung erforderlich, um festzustellen, welche Protokolle in Ihrem Netzwerk verwendet werden und welche gefiltert werden können, ohne dass dadurch Ihr Netzwerksystem beeinträchtigt wird.

6.2.3 Filterung von Netzwerkprotokollen

Wenn Sie vermuten, dass Netzwerkprotokolle die Leistungsfähigkeit Ihres Netzwerks nachteilig beeinflussen, können Sie auf folgende Weise unnötige oder unerwünschte Netzwerkprotokolle ausfiltern.

1. Prüfen Sie, welche Netzwerkstationen und -dienste innerhalb Ihrer Netzwerkumgebung eingesetzt werden.
2. Sehen Sie in der Dokumentation zum Betriebssystem Ihres Netzwerks nach, welche Protokolle die Netzwerkserver, -dienste und (drahtlosen) Stationen benötigen.
3. Starten Sie das RLM Manager-Programm.

4. Markieren Sie das gewünschte Radio Link Module und klicken Sie auf die Schaltfläche **Edit**.
5. Klicken Sie auf die Registerkarte **Bridge**, um die Informationen zur Protokollfilterung anzuzeigen.
6. Klicken Sie rechts oben im Bereich "Protocol filtering" auf die Schaltfläche **Edit**, um das Fenster Protocols to Filter zu öffnen (siehe Abbildung 37 Zu filternde Ethernet-Protokolle auswählen).
7. Aktivieren Sie die Kontrollkästchen der Protokolle, die gefiltert werden sollen.
8. Optional: Wenn Sie ein Protokoll filtern wollen, das nicht in der Liste aufgeführt ist, klicken Sie auf die Schaltfläche **Custom**, und geben Sie das Protokoll von Hand ein.
9. Klicken Sie auf **OK**, wenn Sie alle Eingaben abgeschlossen haben, um zur Registerkarte **Bridge** zurückzukehren.

   Alle von Ihnen gewählten Protokolle und alle von Ihnen manuell eingetragenen benutzerspezifischen Protokolle werden nun in der Liste **Protocol Filtering** aufgeführt.
10. Klicken Sie nochmals auf **OK**, um diese Einstellungen im Access Point RLM zu speichern und zum Hauptfenster des RLM Manager zurückzugelangen.
11. Erstellen Sie, wie in Schritt 4 - Erstellen einer Sicherungsdatei der Konfiguration (Seite 72) beschrieben, eine Sicherheitskopie.

    Wenn Sie aufgefordert werden, einen Namen für die Sicherheitskopie anzugeben, sollten Sie einen Namen wählen, der sich vom Dateinamen der ursprünglichen Konfigurationsdatei unterscheidet. Überschreiben Sie nicht die ursprüngliche Version der Sicherheitskopie,

da Sie sonst Schwierigkeiten bei der Wiederherstellung der ursprünglichen Konfiguration haben könnten, falls die Änderung nicht die erhoffte Leistungssteigerung gebracht hat.

Wiederholen Sie die Schritte wie unter Benötigt Ihr Netzwerk Protokollfilterung? (Seite 130) beschrieben und prüfen Sie nach, ob diese Änderung zu einer Lösung des Problems geführt hat. Wurde das Problem nicht behoben, können Sie eine der folgenden Optionen wählen:

- Optimierung von drahtgebundenen Verbindungen
- Optimierung von drahtlosen Verbindungen

6.2.4 Optimierung von drahtgebundenen Verbindungen

In manchen Fällen ist die mangelnde Leistungsfähigkeit Ihrer (drahtlosen) Verbindung auf einen Fehler der Verkabelung Ihres Netzwerks mit der drahtgebundenen Infrastruktur zurückzuführen.

Solche Fehler können durch eine der folgenden Situationen hervorgerufen werden:

- Fehlerhafte Kabel oder Stecker in der drahtgebundenen Infrastruktur
- Ein Bereich in Ihrem LAN, das sich über eine viel zu lange Entfernung hinzieht.

In diesem Fall kommt es in der Regel zu folgendem Verhalten:

- Das System arbeitet überhaupt nicht mehr, oder

Beseitigung von unnötigem Verkehr

- Ihr Netzwerksystem erzeugt aufgrund der fehlerhaften Verbindung(en) eine große Menge an Fehlermeldungen. Da diese Fehlermeldungen Bandbreite benötigen, kann es zu einem deutlichen Abfall der Netzwerkleistung kommen.

6.2.5 Überprüfen des Kabelsystems

Fehler im Kabelsystem können mittels Remote-Statistik auf der Registerkarte "Remote" im Monitor-Modus des RLM Manager diagnostiziert werden.

1. Wählen Sie **Interface 1: Ethernet** im Pull-Down-Menü, um die Statistik für die Ethernet-Schnittstelle anzuzeigen.
2. Vergleichen Sie die Anzahl der **In errors** mit der Anzahl der **Bridge in packets**.
   - Wenn die Anzahl der “In errors” bei 1% der “Bridge in packets” oder darüber liegt, kann dies auf ein Problem im Kabelsystem hindeuten.
3. Vergleichen Sie die Anzahl der **Out errors** pakets mit der Anzahl an **Bridge out packets**.
   - Wenn die Anzahl der “Out errors” bei 1% der “Bridge out packets” oder darüber liegt, kann dies auf ein Problem im Kabelsystem hindeuten.
4. Vergleichen Sie die Anzahl der **Out carrier sense errors** mit der Anzahl der **Bridge out packets**.

- Wenn die Zahl der “Out carrier sense errors” bei 1% der “Bridge out packets” liegt oder der Wert für die “Out carrier sense errors” zu rasch steigt, deutet dies auf mangelnde Platzressourcen im Netz aufgrund einer Backbone-Überlastung oder eines Kabelproblems hin.

5. Überprüfen Sie, ob das Problem nur beim gewählten RLM oder bei mehreren Access Points (RLMs) auftritt.
   - Tritt das Problem nur an einem Access Point RLM, kann die Ursache an den Steckern oder Kaberverbindungen zwischen dem Radio Link Module und dem Hub bzw. dem drahtgebundenen Backbone liegen.
   - Tritt das Problem an mehreren Access Points (RLMs) auf, liegt die Ursache wahrscheinlich an den Kabeln oder Steckern der drahtgebundenen Backbones, Hubs oder Bridge/Router, die diesen Netzbereich mit Ihrem LAN verbinden.

6.2.5.1 Problembehandlung bei Fehlern im Kabelsystem

Wenn Sie die oben beschriebenen Schritte ausgeführt haben, sollten Sie in der Lage sein, den Bereich zu finden, in dem das Kabelproblem lokalisiert ist. Um das Problem zu beseitigen sollten Sie das Kabelsystem im fehlerverdächtigen Bereich vorsichtig überprüfen und sich vergewissern, dass alle Stecker ordnungsgemäß verbunden sind mit:

- Access Points (RLMs)
- den Bridges, Routern und Hubs
- den drahtgebundenen Stationen, die an das Kabelsystem angeschlossen sind.

Wenn in Ihrem Netzwerk BNC-Koax-Kabel (10Base2) verwendet werden, vergewissern Sie sich, dass die Anschlüsse auf beiden Seiten ordnungsgemäß ausgeführt sind.

6.2.6 Überprüfung der Länge Ihrer LAN-Bereiche

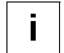
In seltenen Fällen können Netzwerkprobleme auch auf zu lange LAN-Bereiche zurückzuführen sein.

Hierbei kann es zu häufigen Kollisionen am Ethernet Interface kommen. Kollidierte Telegramme werden von den Zielstationen nicht mehr empfangen.

Überdimensionierte LAN-Bereiche können mittels Remote-Statistik auf der Registerkarte **Remote** im Monitor-Modus des RLM Manager diagnostiziert werden.

1. Wählen Sie **Interface 1: Ethernet** im Pull-Down-Menü, um die Statistik für die Ethernet-Schnittstelle anzuzeigen.
2. Vergleichen Sie die Anzahl der **In errors** mit der Anzahl der **Bridge in packets**.
   - Wenn die Anzahl der **In errors** bei 1% der **Bridge in packets** oder darüber liegt, kann dies auf ein Problem im Kabelsystem hindeuten.
3. Beobachten Sie die Erhöhung des Parameters **Bytes in** über einen längeren Zeitraum.
   - Steigt der Wert konstant mit über 600,000 Bytes pro Sekunde, kann dies auf eine übermäßige Länge Ihres LAN-Bereichs hindeuten.

Unter Umständen sollten Sie einen Netzwerkexperten hinzuziehen, damit die Länge Ihrer Kabel-Sgmente überprüft und / oder korrigiert wird.



HINWEIS:

Wenn Sie den LAN-Bereich in mehrere Teilbereiche aufsplitten, vergewissern Sie sich, dass alle Geräte mit SIMATIC NET IWL im gleichen LAN-Bereich gruppiert bleiben, da die drahtlosen Stationen nicht zwischen LAN-Bereichen mobil werden können, die über Router oder Gateways getrennt sind.

Wurde das Problem nicht behoben, können Sie eine der folgenden Optionen in diesem Kapitel wählen

- Protokollfilterung (Seite 129)
- Optimierung von drahtlosen Verbindungen (Seite 138)

6.2.7 Optimierung von drahtlosen Verbindungen

Ist die Verbindungsqualität zwischen einer drahtlosen Station und dem Access Point RLM beeinträchtig, kann es zu einem Verlust der Pakete kommen, die zwischen dieser Station und dem Radio Link Module ausgetauscht werden. Wartet die sendende Station vergeblich auf eine Empfangsbestätigung der empfangenden Station, überträgt erstere das verlorengegangene Paket ein zweites Mal.

Nachdem die Empfangsstation das gleiche Paket ein zweites Mal erhält, entscheidet sie sich möglicherweise dazu, alle bis zu diesem Zeitpunkt empfangenen Pakete zu verwerfen, so dass die sendende Station alle Pakete erneut übertragen muss .

Bitte beachten Sie:

- Die vielen wiederholten Übertragungen können sich negativ auf Ihren Datendurchsatz auswirken, da die “echten Daten” die verfügbare Bandbreite mit den wiederholt gesendeten Telegramm teilen müssen.
- Die Übertragungswiederholungen beeinträchtigen auch die Leistungsfähigkeit, so wie diese vom Endbenutzer einer drahtlosen Station wahrgenommen wird: z.B., dauert für den Benutzer das Speichern einer Datei länger.

Zu einer Beeinträchtigung der Verbindungsqualität kann es aus einem der folgenden Gründe kommen:

- Die Station befindet sich fast ausser Reichweite des Access Point RLM.
- Es gibt eine Störquelle zwischen der Station und dem Radio Link Module.
- Eine Station kann möglicherweise von einer anderen Station innerhalb des gleichen Funkabdeckungsbereichs ”verdeckt” werden (weitere Informationen zu verdeckten Stationen finden im Abschnitt RTS/CTS-Medienreservierung (Seite 145)).

6.2.8 Diagnose der Verbindungsqualität

Im drahtlosen Netzwerk kann die Beeinträchtigung der Verbindungsqualität auf unterschiedliche Weise diagnostiziert werden.

- Verwenden Sie das RLM Manager-Tool, um die Qualität der Funkverbindung vor Ort wie unter Überwachen des SIMATIC NET IWL-Netzes (Seite 73) beschrieben zu diagnostizieren, oder
- Verwenden Sie das RLM Manager-Tool um herauszufinden, ob bestimmte abgesetzte Bereiche eine beeinträchtigte Leistung aufweisen .

  Der RLM Manager bietet folgende Optionen, um die Qualität von Funkverbindungen zu diagnostizieren:

  - Remote Link-Test
  - Registerkarte "Wireless"
  - Registerkarte "Remote"

Anhand dieser Parameter läßt sich feststellen, ob die schlechten Leistungswerte Ihres Netzwerks durch Störungen hervorgerufen wird.

6.2.8.1 Remote Link-Test

Weitere Informationen zum Fenster Remote Link-Test, in dem Verbindungen anhand von dynamischen Indikatoren darstellt werden, erhalten Sie unter Fenster Remote Link Test (Seite 112).

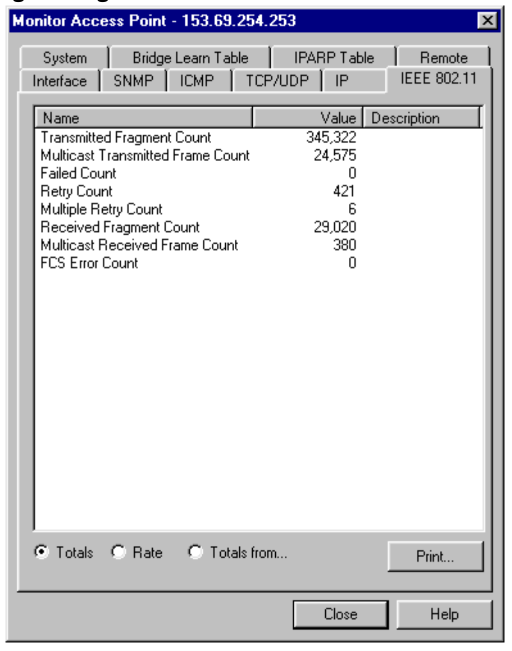
Wichtige Indikatoren, die im Fenster Remote Link-Test überwacht werden können sind:

- Das Signal-/Rauschverhältnis (SNR), das die Funkverbindungsqualtität im Überblick zeigt.
- Der Signalpegel, um festzustellen, ob das beeinträchtigte SNR mit dem schwachen Funksignal zusammenhängt (Station ausserhalb des Empfangsbereiches).
- Der Rauschpegel, um festzustellen, ob das beeinträchtigte SNR mit einer Störquelle zusammenhängt.

6.2.8.2 IEEE-Information

Die IEEE-Information auf der Registerkarte **IEEE 802.11** im Monitor-Modus erlaubt es, die Telegrammaktivität auf der Funk-LAN Schnittstelle des Access Point RLM zu verfolgen.

Abbildung 23 Registerkarte IEEE information



Es gibt drei wichtige Indikatoren, die Sie besonders im Auge behalten sollten sind:

- **Retry Count** - zählt die Telegramme, die bei Übertragungsbeginn aufgrund von Kollisionen verlorengehen. Im Normalbetrieb sollte der Wert für **Retry Count** weniger als 3% des Wertes für **Transmitted Fragment Count** betragen.
- **Multiple Retry Count** - zählt die Telegramme, die nach Übertragungsbeginn aufgrund von Kollisionen verlorengehen. Im Normalbetrieb liegt der Wert für **Multiple Retry Count** bei weniger als 3% des Wertes für **Retry Count**.
- **Failed Count** - zählt die Telegramme, die den Wert **Retry Limit** erreicht haben. Es wir nicht mehr versucht, fehlgeschlagene Telegramme zu übertragen.

  Liegt der Wert für **Failed Count** bei 1% des Wertes für **Multiple Retry Count** oder darüber, wird Ihr Netzwerk möglicherweise durch Störungen beeinträchtigt. Um den Störungsgrund festzustellen, verwenden Sie das RLM Manager Fenster Remote Link Test (Seite 112). Achten Sie dabei auf eine plötzliche Erhöhung der Rauschwerte bzw. auf niedrige SNR-Werte.

6.2.8.3 Remote-Statistik-Parameter

Wählen Sie die Registerkarte **Remote** im Monitor-Modus. Wählen Sie eine Schnittstelle aus dem Pull-Down-Menü, um die Statistiken für die drahtlosen Netzwerkschnittstellen anzuzeigen. Führen Sie anschließend die folgenden Schritte aus, um die Verbindungsqualität zu diagnostizieren:

1. Vergleichen Sie die Anzahl der **In errors** mit der Anzahl der **Bridge in packets**.

- Wenn die Anzahl der “In errors” bei 1% der “Bridge in packets” oder darüber liegt, kann dies auf ein hohes Verkehrsaufkommen im drahtlosen Medium hindeuten.

2. Um diese Vermutung zu bestätigen, vergleichen Sie anschließend die Anzahl der “Out errors” pakets mit der Anzahl der “Bridge out packets”.
   - Wenn die Anzahl der **Out errors** bei 1% der **Bridge out packets** oder darüber liegt, kann davon ausgegangen werden, dass die Verbindungsqualität bei einer oder mehreren Stationen beeinträchtigt ist.
3. Vergleichen Sie die Anzahl der **Out collisions** packets mit der Anzahl der **Bridge out packets**.
   - Wenn die Anzahl der **Out collisions** bei 1% der **Bridge out packets** oder darüber liegt, kann mit hoher Wahrscheinlichkeit von einem starken Verkehrsaufkommen im drahtlosen Medium ausgegangen werden. Dies könnte an den zahlreichen Telegrammen liegen, die jeweils mehrmals übertragenen werden - oder aber auch auf gleichzeitige Verbindungsversuche mehrerer Stationen zurückzuführen sein.
4. Sie können auch den Remote Link-Test des RLM Manager verwenden, um festzustellen, ob bei einer oder mehreren Stationen eine schlechte Verbindungsqualität zu beobachten ist:
   - Wenn die schlechte Verbindungsqualität durch einen niedrigen Signalpegel hervorgerufen wird, befindet sich die Station fast ausserhalb der Reichweite des Access Point RLM.

- Wenn die schlechte Verbindungsqualität durch einen hohen Rauschpegel hervorgerufen wird, so deutet dies auf eine Störquelle zwischen der Station und dem Radio Link Module hin.

5. Wenn eine oder mehrere Stationen eine schlechte Verbindungsqualität aufweisen, -führt die wiederholte Übertragung von Telegramme zu einer allgemeinen Beeinträchtigung der Statistiken und der Leistungsfähigkeit.
   - Sie können das Problem möglicherweise lösen, indem Sie die Station(en) verlagern oder die Störquelle beseitigen.
   - Ist das Problem auf ein schwaches Signal zurückzuführen, können Sie:
   - — ein Antenne an die betroffenen Stationen oder Access Points anschliessen, um eine Erhöhung der Reichweite zu erreichen.
   - — ein zusätzliches Access Point RLM in Ihr Netzwerk implementieren
   - — die Positionen Ihrer Access Points (RLMs) anpassen, um eine ausreichende Funkabdeckung für alle drahtlosen Stationen zu gewährleisten.
   - Wenn Sie eine "verdeckte" Station vermuten, lesen Sie RTS/CTS-Medienreservierung (Seite 145).



HINWEIS:

Sie können auch den CP 1515 Manager verwenden, um die Verbindungsqualität zwischen einer abgesetzten Station und dem Access Point RLM zu analysieren. Hierbei ist der Zugang zum Fehlerort erforderlich, da die Diagnose Vor Ort vorgenommen werden muss.

Wurde das Problem nicht behoben, können Sie eine der folgenden Optionen wählen

- Protokollfilterung (Seite 129)
- Optimierung von drahtgebundenen Verbindungen (Seite 133)
- Aufbau von Hochleistungsnetzen (Seite 162)

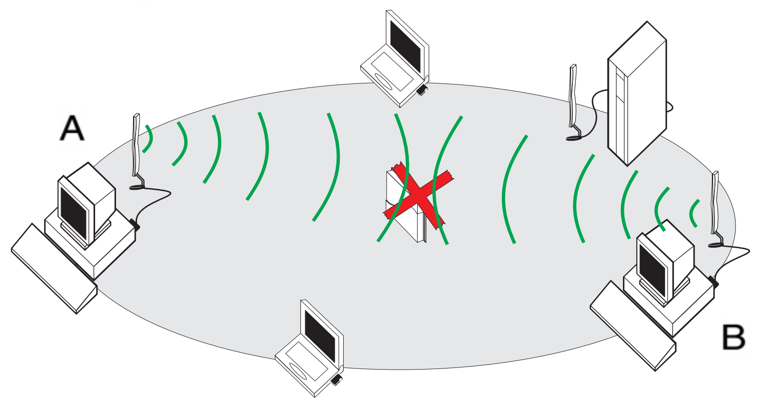
6.2.8.4 RTS/CTS-Medienreservierung

Stellt eine SIMATIC NET IWL-Station fest, dass ein weiteres drahtloses Gerät das drahtlose Medium benutzt, so verzögert diese automatisch die anstehenden Übertragungen.

Dieses standardmäßige Verhalten - auch als CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)-Protokoll bekannt - verhindert die Kollision drahtloser Telegramme im Falle dass zwei oder mehr Stationen Ihre Datenübertragung gleichzeitig starten.

Dank der RTS/CTS-Medienreservierung kann die Funkleistung auch in Netzwerkumgebungen verbessert werden, in denen das CSMA/CA-Protokoll aufgrund des in Abbildung 24 Das Problem der verdeckten Stationen dargestellten Problems der "verdeckten Stationen" versagen würde.

Abbildung 24 Das Problem der verdeckten Stationen



Die RTS/CTS-Medienreservierung kann eine Lösung für Netzwerke bieten in denen:

- Die Dichte der Stationen und Access Points (RLMs) sehr gering ist.
- eine geringe Netzwerkleistung aufgrund der überhöhten Anzahl an Framekollisionen an den Zugangspunkten Access Points (RLMs) festzustellen ist.

6.2.8.5 Über das Problem der verdeckten Stationen

Das Problem der verdeckten Station tritt dann auf, wenn zwei drahtlose Stationen sich im Empfangsbereich des gleichen Access Point RLM befinden, aber keine Daten untereinander austauschen können.

Abbildung 24 Das Problem der verdeckten Stationen stellt das Problem der verdeckten Stationen dar. Die Stationen A und B befinden sich beide innerhalb des Empfangsbereiches des Access Point RLM. Dennoch kann Station B keine Daten von Station A empfangen. Aus der Sicht von Station B ist Station A daher eine verdeckte Station.

Startet Station B eine Übertragung zum Radio Link Module, merkt sie möglicherweise nicht, dass Station A bereits das drahtlose Medium benutzt. Wenn Station A und Station B zur gleichen Zeit Telegramme senden, kann es zu einer Kollisionen kommen, wenn diese im selben Moment am Access Point RLM eintreffen. Die Kollision führt mit hoher Wahrscheinlichkeit zu einem Nachrichtenverlust für beide Stationen.

Bei Szenarien wie sie in Abbildung 24 Das Problem der verdeckten Stationen dargestellt sind, kann die RTS/CTS-Medienreservierung eine Lösung bieten, indem sie die Übertragungssteurung an den Access Point RLM überträgt.

Bei der Problembehandlung sollten sich die Massnahmen auf die betroffenen Stationen selbst konzentrieren, die aufgrund des Problems mit verdeckten Stationen fehlerhaft arbeiten - auf diese Weise lassen sich die besten Ergebnisse erzielen.

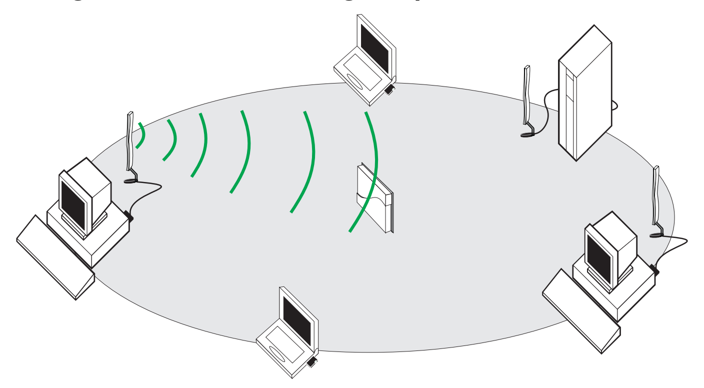
Bei der Konfiguration der PC Card CP 1515-Parameter einzelner Stationen kann die RTS/CTS-Medienreservierung aktiviert werden:

- Um den Parameter RTS/CTS-Medienreservierung zu aktivieren, wählen Sie **Add/Edit configuration profile** im CP 1515 Manager, wählen Sie anschließend die Registerkarte **Advanced** und aktivieren Sie **RTS/CTS Medium Reservation**.

Beseitigung von unnötigem Verkehr

Die RTS/CTS-Medienreservierung läßt sich individuell für jede Station einstellen, d.h., die Konfiguration dieses Parameters muss nicht die gleiche für alle Geräte in Ihrem Netzwerk sein, die mit SIMATIC NET IWL ausgerüstet sind.

Abbildung 25 Medienreservierung "Request to Send"



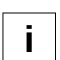
6.2.8.6 So funktioniert die Medienreservierung

Sobald Sie die RTS/CTS-Medienreservierung auf einer verdächtigen Station aktivieren, verwendet diese Station und dessen Access Point RLM das RTS/CTS-Protokoll (Request to Send/Clear to Send protocol).

- Die Station richtet eine RTS-Anfrage an das RLM, in der auch Informationen zur Telegrammlänge der angefragten Übertragung enthalten sind (siehe Abbildung 25 Medienreservierung “Request to Send”).
- Sobald das Access Point RLM die Anfrage erhält, sendet es eine CTS-Telegramm an alle Stationen, die sich in seinem Empfangsbereich befinden, um:
  - alle anderen Stationen zu veranlassen, ihre Übertragungen um den Zeitrahmen der angefragten Übertragung zu verzögern.
  - der anfragenden Station zu bestätigen, dass das Access Point RLM die Verfügbarkeit des Mediums geprüft hat und entsprechende Ressourcen für die angefragte Übertragung reserviert hat.

  Der CTS-Prozess wird in Abbildung 26 Medienreservierung “Clear to Send” dargestellt.

Abbildung 26 Medienreservierung “Clear to Send”



HINWEIS:

In den meisten Netzwerkumgebungen ist in der Regel keine Aktivierung der RTS/CTS-Medienreservierung am Access Point RLM erforderlich, um Kollisionen zu vermeiden.

Dies liegt daran, dass alle am Access Point RLM angeschlossenen Stationen sich normalerweise im Empfangsbereich dieses Radio Link Module befinden und daher feststellen können, ob und wann das RLM das drahtlose Medium zur Nachrichtenübertragung nutzt.

Bei einer Aktivierung der RTS/CTS-Medienreservierung am RLM würde das Access Point RLM ein CTS für jedes Telegramm an Stationen innerhalb seines Funkbereiches benötigen - selbst wenn es sich um Verkehr zwischen Stationen ein und derselben Funkzelle handelt.

Dies könnte zu einer unnötigen Belastung des Netzes führen und die Durchsatzleistung, statt eine Lösung zu bieten.

Wenn Sie dennoch die RTS/CTS-Medienreservierung am Access Point RLM aktivieren, werden Sie feststellen, dass die Konfiguration dieser Option für Access Points (RLMs) leicht von der Konfiguration für den CP 1515 in einer Station abweicht.

Anhand der Access Points (RLMs) läßt sich die Empfindlichkeit des RTS/CTS-Mechanismus individuell einstellen. Durch Eingabe eines benutzerdefinierten Wertes für die Telegrammlänge im Feld **RTS/CTS Medium Reservation Threshold** (wählen Sie die Registerkarte **Interface** im Edit Mode und klicken Sie anschließend auf die Schaltfläche **Advanced**), können Sie darauf Einfluss nehmen, in welchen Fällen das Access Point RLM den RTS/CTS-Mechanismus einsetzt. Zum Beispiel:

- Ist eine Telegramm kürzer als der Schwellwert der RTS/CTS-Medienreservierung, sendet das Access Point RLM keine RTS-Anfrage an die Zielstation und benutzt statt dessen das CSMA/CA-Protokoll: d.h., das Telegramm wird ohne Verzögerung übertragen, sobald das Medium frei ist.
- Ist ein Telegramm dagegen länger als der Schwellwert der RTS/CTS-Medienreservierung, sendet das Access Point RLM zunächst eine RTS-Anfrage an die Zielstation und verzögert die Übertragung bis die Zielstation mit einer CTS-Telegramm antwortet.

Alle anderen Stationen werden ihre Übertragungen für die Dauer der in der CTS-Telegramm angegeben "Funkverbotsdauer" verzögern.

6.2.8.7 RTS/CTS-Medienreservierung

1. Starten Sie das RLM Manager-Programm, wählen Sie das Radio Link Module, das die Funkzelle bedient in der Sie eine beeinträchtigte Leistungsfähigkeit aufgrund einer verdeckten Station vermuten und klicken Sie auf die Schaltfläche **Edit**.
2. Wählen Sie die Registerkarte **Wireless Interfaces**.
3. Wählen Sie den Socket in dem sich die Netzschnittstelle befindet, die von einer verdeckte Station betroffen ist.
4. Klicken Sie auf die Schaltfläche **Advanced**.
5. Klicken Sie auf das Kontrollkästchen **RTS/CTS Medium Reservation**.
6. Geben im Feld **Threshold** einen Wert zwischen 0 und 2347 ein.

   Die Standardeinstellung für den Schwellwert der RTS/CTS-Medienreservierung ist 2347 (deaktiviert) - RTS/CTS wird nicht verwendet.

   - In einem Netzwerk mit aktivierter RTS/CTS-Medienreservierung beträgt der typische Wert für die Medienreservierung 500.
   - Sie können alternativ einen anderen Wert eingeben.

   Der hier eingegebene Wert entscheidet darüber, wann das Access Point RLM eine RTS-Telegramm sendet. Beträgt der gewählte Wert z.B. 500, so:

   - veranlasst das RLM eine Aktivierung des RTS/CTS-Protokolls für jedes Telegramm mit einer Länge über 500.

- werden Telegramme mit einer Länge unter 500 mithilfe des CSMA/CA-Standardprotokolls übertragen.

7. Klicken Sie auf **OK**, um zur Registerkarte Interface zurückzukehren.
8. Klicken Sie erneut auf **OK**, um die neue Konfiguration für das Access Point RLM zu speichern und kehren Sie zum Hauptfenster des RLM Manager zurück.
9. Erstellen Sie eine Sicherheitskopie der neuen Konfiguration (siehe Schritt 4 - Erstellen einer Sicherungsdatei der Konfiguration (Seite 72)).

6.2.8.8 Verwaltung der Frequenzkanäle

Setzt sich Ihr Netzwerk aus mehr als einem Access Point RLM zusammen, empfiehlt es sich, die Unterkanalfrequenzen zwischen benachbarten Access Points (RLMs) unterschiedlich einzustellen, um eine höhere Bandbreite für die drahtlosen Stationen der unterschiedlichen Zellen bereitzustellen.

Die Anzahl der verfügbaren Kanälen hängt von Ihren landesspezifischen Fernmeldebestimmungen ab. Im Handbuch "Industrial Ethernet Wireless LAN Grundlagen" sowie auf der MOBIC Webseite **http://www.siemens.com/mobic** finden Sie eine Liste der landesspezifisch zugelassenen Kanäle.

6.2.8.9 Zweikanalkonfiguration

Ein Zweikanal-System kann wie folgt aussehen:

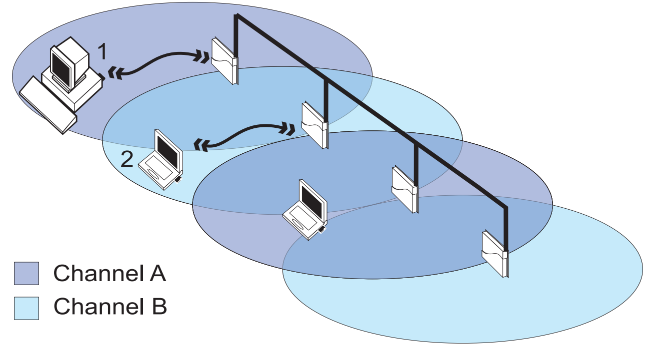
- Alle Access Point RLMs, die auf Kanal A senden benutzen Kanal 1 (2412 MHz).

Beseitigung von unnötigem Verkehr

- Alle Access Point RLMs, die auf Kanal B senden benutzen Kanal 11 (2462 MHz).



Abbildung 27 Zweikanal-Konfiguration



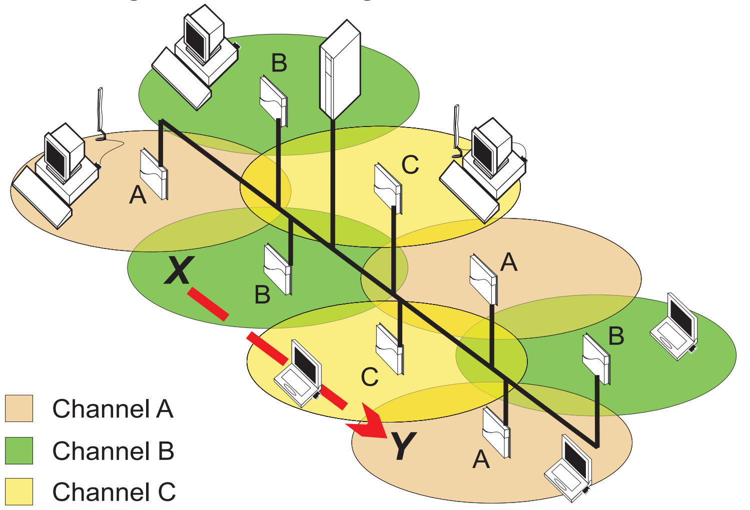
Auf diese Weise können Sie einen maximalen Kanalabstand für banachbarte Access Points (RLMs) einstellen und die Anforderungen für einen optimalen Betrieb mühelos einhalten.

Station 1 kummuniziert mit seinem Access Point RLM über Kanal A, ohne dass dadurch Station 2 die Übertragungen zum benachbarten Radio Link Module verzögern muss. Wandert eine der beiden Stationen zu einem anderen Standort, wechselt sie automatisch die Funkfrequenz auf einen beliebigen Kanal, um mit dem Netzwerk in Verbindung zu bleiben.

6.2.8.10 Mehrkanalkonfiguration

Bei den Frequenzkanälen Ihres Access Points (RLMs) können Sie zwischen drei oder mehr Unterkanälen wechseln (entsprechend Ihren landesspezifischen Fernmeldebestimmungen).

Abbildung 28 Mehrkanalkonfiguration



Zum Beispiel läßt sich entsprechend Mehrkanalkonfiguration (Seite 155) ein Dreikanal-System einrichten, bei dem die Access Points (RLMs) wie folgt konfiguriert sind:

Beseitigung von unnötigem Verkehr

- Alle Access Points (RLMs), die auf Kanal A senden benutzen Kanal 1 (2412 MHz)
- Alle Access Points (RLMs), die auf Kanal B senden benutzen Kanal 6 (2437 MHz),
- Alle Access Points (RLMs), die auf Kanal C senden benutzen Kanal 11 (2462 MHz)

Auf diese Weise kann der minimale Kanalabstand von 25 MHz für benachbarte Radio Link Modules eingehalten werden, der für einen optimalen Betrieb empfohlen wird.

Eine Station, die vom Standort *X* zum Standort *Y* wandert, wechselt automatisch nacheinander von Kanal A nach B und dann nach C, um am Netz angeschlossen zu bleiben.

In diesem Fall müssen jeder CP 1515 im RLM unterschiedliche Frequenzkanäle zugewiesen werden (mit einem Abstand von 25 MHz oder mehr), um Wechselkommunikation zwischen zwei Karten zu verhindern.

6.2.8.11 Konfiguration der Kanalfrequenz

Um die Frequenz Ihres Access Point RLM zu wechseln, gehen Sie wie folgt vor:

1. Stellen Sie eine Verbindung zum RLM her, indem Sie den RLM Manager öffnen und ein Ziel- Access Point RLM wählen. Anschliessend klicken Sie auf die Schaltfläche **Edit**.
2. Wählen Sie die Registerkarte **Wireless Interfaces**.
3. Wählen Sie den Socket (A oder B) für die Netzschnittstelle, die Sie konfigurieren wollen.

4. Klicken Sie auf die Schaltfläche **Advanced**. Die PC Card CP 1515 unterstützt unterschiedliche Unterkanäle (im Pull-Down-Menü können Sie eine andere Betriebsfrequenz wählen). Die Anzahl der Kanäle hängt von den entsprechenden landesspezifischen Bestimmungen ab.
5. im Fenster Wireless Advanced Setup können Sie anhand des Pull-Down-Menüs **Channel** einen Unterkanal wählen, um den maximalen Kanalabstand zu benachbarten Access Points (RLMs) zu erreichen (Mindestkanalabstand: 25 MHz).

   Tabelle 2Empfohlene Unterkanal-Konfigurationen zeigt bewährte Kanalkombinationen, die Sie bei der Konfiguration von SIMATIC NET IWL-Neztwerken mit mehreren Radio Link Modules verwenden können.

   - Bei der Zweikanalkonfiguration (Seite 153), wechseln Sie zwischen den Kanälen A und B.
   - Bei der Mehrkanalkonfiguration (Seite 155), wechseln Sie zwischen den Kanälen A, B und C



HINWEIS:

Die Anzahl der verfügbaren Kanäle in Tabelle 2Empfohlene Unterkanal-Konfigurationen hängt von Ihren landesspezifischen Fernmeldebestimmungen ab. Im Handbuch "Industrial Ethernet Wireless LAN Grundlagen" sowie auf der MOBIC Webseite
http:\\www.siemens.com\mobic
finden Sie eine Liste der landesspezifisch zugelassenen Kanäle.

Tabelle 2 Empfohlene Unterkanal-Konfigurationen

Kanal A	Kanal B	Kanal C
2412 MHz (1)	2437 MHz (6)	2462 MHz (11)

Bei drahtlosen Neztwerken, in denen sich die Funkzellen nur leicht überlappen, können Sie auch mit der Mehrkanalkonfiguration experimentieren und einen Kanalabstand von weniger als 25 MHz wählen - dazu können Sie z.B., die Kanäle in Tabelle 3 Optionale Unterkanal-Konfigurationen verwenden.

Tabelle 3 Optionale Unterkanal-Konfigurationen

Kanal A	Kanal B	Kanal C	Kanal D
2412 MHz (1)	2427 MHz (4)	2442 MHz (7)	2457 MHz (10)

6. Klicken Sie auf **OK** um das Fenster Wireless Advanced Setup zu schliessen und kehren Sie zur Registerkarte **Wireless Interfaces** zurück.
7. (Optional) Wiederholen Sie die Schritte 3 bis 6 um die Frequenz für die zweite Netzschnittstelle dises Access Point RLM zu überprüfen bzw. zu ändern.
8. Klicken Sie erneut auf **OK**, um die neue Konfiguration für das Radio Link Module zu speichern und kehren Sie zum Hauptfenster des RLM Manager zurück.
9. Erstellen Sie eine Sicherheitskopie der neuen Konfiguration (siehe Schritt 4 - Erstellen einer Sicherungsdatei der Konfiguration (Seite 72)).
10. Tragen Sie den "Access Point Configuration Record" in A "Startkonfiguration" ein, um diese Änderungen zu aktualisieren.
11. (Optional) Ändern Sie die Konfiguration aller anderen Access Points (RLMs) entsprechend. Es wird empfohlen unterschiedliche Frequenzen für benachbarte Radio Link Modules zu verwenden - siehe dazu Zweikanalkonfiguration (Seite 153) oder Mehrkanalkonfiguration (Seite 155).

6.2.9 Link Integrity

Bei einer Unterbrechung der Verbindung zwischen dem Access Point RLM und dem restlichen Ethernet-Netzwerk (in der Regel geschieht dies aufgrund einer fehlerhaften Kabelverbindung oder eines Netzwerkfehlers), kommt es zu einer Störung der normalen Netzkommunikation zwischen den mobilen drahtlosen Stationen.



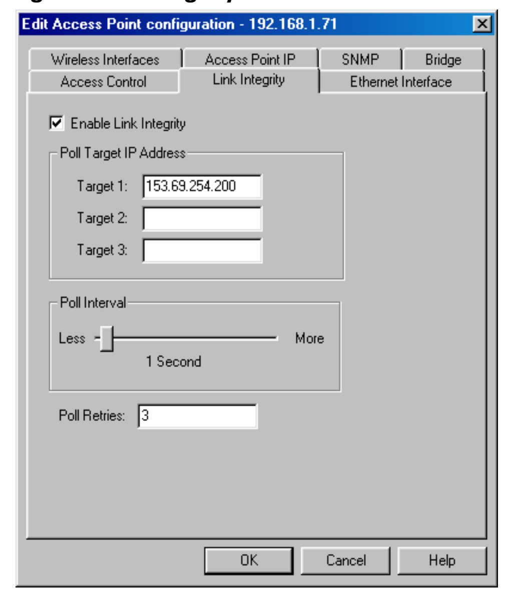
ACHTUNG:
Diese Funktion kann zur Erhöhung der Zuverlässigkeit genutzt werden, wenn ein zweiter Acesspoints RLM vom ersten RLM und der mobilen Station erreicht werden kann.

Ist die drahtlose Verbindung noch funktionsfähig, wandert die drahtlose Station nicht zu einem anderen Access Point RLM, da die "physikalische" Verbindung zum Access Point RLM als “gut” oder “ausreichend” empfunden wird.

Das Ethernet link integrity-Feature ist eine High-End-Lösung speziell für diese Art von Netzwerkfehlern, da es den Access Points (RLMs) ermöglicht:

- Verbindungsstörungen zu den Netzdiensten festzustellen, indem es die Verbindung zwischen dem RLM und einem Maximum von drei IP hosts testet.
- die Verbindung automatisch mit einem anderen Access Point RLM wieder herzustellen, wenn die Störung nicht auf schlechte Funkqualität zurückzuführen ist .

Abbildung 29 Link Integrity-Fenster



Weitere Informationen zum Thema Link Integrity finden Sie in der Hilfe-Datei des RLM Manager-Programms.

6.3 Aufbau von Hochleistungsnetzen

Falls der Datenbedarf der Benutzer in Ihrer Netzwerkumgebung sehr hoch ist, oder falls sich in Ihrer Netzwerkumgebung auf kleiner Fläche sehr viele Benutzer befinden, kann es unter Umständen sinnvoll sein, die Datendurchsatz durch Lastenverteilung Ihrer Access Point RLMs zu verbessern.

Die hier beschriebene Lösung ermöglicht es Ihnen, einen Mittelweg zu finden zwischen "maximaler Reichweite bei minimalen Hardware-Investitionen" und "maximalem Datendurchsatz bei höheren Hardware-Investitionen".

6.3.1 Über das CSMA/CA-Protokoll

In normalen Netzwerk-Konfigurationen verwenden alle Geräte ein Standardmechanismus, um Kollisionen bei drahtlosen Telegramme zu vermeiden. Beabsichtigt eine Station eine Telegramm zu senden, so prüft sie daher zuerst, ob es andere Stationen gibt, die bereits Telegramme übertragen (über das drahtlose Medium).

- Wenn aktuell keine anderen Übertragungen stattfinden, startet die Station ihre eigene Übertragung.
- Stellt sie dagegen fest, dass bereits Übertragungen im Gange sind, wird ein zufallsgesteuerter Verzögerungstimer eingesetzt. Nach Ablauf des Timers, prüft die Station erneut das Medium, um festzustellen ob sie mit ihrer Übertragung beginnen kann.

Dieses Protokoll, auch CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)-Protokoll genannt, eignet sich bestens für die meisten

Netzwerkumgebungen. Für den Benutzer eines drahtlosen Gerätes ist das Verzögerungsverhalten dabei kaum spürbar.

In Netzwerkumgebungen mit vielen dichtgedrängten drahtlosen Benutzern und / oder drahtlosen Stationen mit hohem Datenverkehrsaufkommen, kann es bei den drahtlosen Stationen zu einer Beeinträchtigung der Leistungsfähigkeit kommen, die sich in langen Netzreaktionszeiten bei der Kommunikation mit dem Netzwerk bemerkbar macht.

Während eine Beeinträchtigung der Leistungsfähigkeit normalerweise durch die schlechte Qualität von Funkverbindungen hervorgerufen wird (sichtbar am schlechten Signal-/Rauschverhältnis), kann das oben beschriebene Szenarium auch in Fällen auftreten, bei denen:

- Site Monitor Messungen eines CP 1515 Managers, eine exzellente drahtlose Abdeckung durch mindestens zwei oder mehr Access Points (RLMs) an jedem Standort ergeben.
- Übertragungsmessungen an diesen Standorten:
  - zeigen ein exzellentes Signal-/Rauschverhältnis (SNR) für den Datenaustausch zwischen drahtlosen Stationen und dem Radio Link Module.
  - zeigen eine große Anzahl an Telegrammen (Receive Messages), die mit niedriger Geschwindigkeit übertragen werden.

In diesen Fällen wird die unzureichende Netzwerkleistung unter Umständen durch das starke drahtlose Verkehrsaufkommen in Bereichen hervorgerufen, in denen die Stationen aufgrund des CSMA/CA-Protokolls Ihre Übertragungen zu oft verzögern müssen, weil:

- es starken Datenverkehr anderer Stationen in der gleichen drahtlosen Zelle gibt

- es Verkehr von Stationen benachbarter Zellen gibt, wobei Stationen in Standorten bei denen sich die drahtlosen Zellen überlappen eher betroffen sind.

Der letztgenannte Fall ist normalerweise nur in Netzwerken anzutreffen, bei denen alle Access Points (RLMs) so konfiguriert sind, dass sie entweder mit der gleichen Frequenz arbeiten oder mit Frequenzen, die keinen ausreichenden Abstand zwischen den Kanälen bieten (siehe Verwaltung der Frequenzkanäle (Seite 153)).

6.3.1.1 Steuerung des Verzögerungsverhaltens

Um das oben beschriebene Leistungsproblem zu beheben, läßt sich auch ein Hochleistungsnetzwerk nach folgendem Schema aufbauen:

- Erhöhen Sie die Anzahl der Radio Link Modules in Ihrem Netzwerk.
- Konfigurieren Sie die Access Points (RLMs) benachbarter Zellen so, dass ein Betrieb auf unterschiedlichen Frequenzkanälen mit maximalem Kanalabstand ermöglicht wird (siehe Verwaltung der Frequenzkanäle (Seite 153).
- Passen Sie den Parameter **Distance Between APs**an, um einen optimalen Lastenausgleich der drahtlosen Stationen pro Access Point RLM zu erreichen (siehe Abstand zwischen Access Points (APs) (Seite 216).



ACHTUNG:
Der Parameter Distance between APs muss sowohl für die drahtlosen Stationen als auch für das Access Point RLM eingerichtet werden. Die eingestellten Werte müssen für

alle drahtlosen Geräte in Ihrem Netzwerk gleich sein, um Unregelmäßigkeiten im Netzwerkverhalten und bei der Roaming-Konnektivität der drahtlosen Geräte zu vermeiden.

Wenn Sie den Parameter **Distance between APs** von **Large** auf **Medium** oder **Small** ändern, können Sie die Empfangsempfindlichkei der RLMs wie folgt reduzieren:

- Die Stationen werden Ihre Roamingaktivitäten intensivieren und sich schneller als bisher an eines der zusätzlichen Access Points (RLMs) anschliessen.
- Dank der zusätzlichen Access Points (RLMs) muss das Verzögerungsverhalten nicht mehr so streng wie in Umgebungen mit einer relativ geringen Dichte an installierten Radio Link Modules sein:
  - Die Stationen verzögern ihre Übertragungen nur, wenn der Signalpegel einer im drahtlosen Medium festgestellten Telegramm einem bestimmten Niveau entspricht oder diesen übersteigt.
  - Es ist unwahrscheinlich, dass Telegramm mit einem niedrigen Signallpegel an das Access Point RLM gesendet werden, das die lokale Zelle bedient, da die Station aufgrund des aktiveren Roaming-Verhaltens in der Regel eine Verbindung zu einen anderen RLM suchen wird.

Um das aktivere Roaming-Verhalten der drahtlosen Stationen zu unterstützen und um die geringere Empfangsempfindlichkeit zu kompensieren, sollte die Änderung des Parameters Distance between APs entsprechend der gestiegenen Anzahl und der dichteren Verteilung Ihrer Access Points (RLMs) vorgenommen werden.

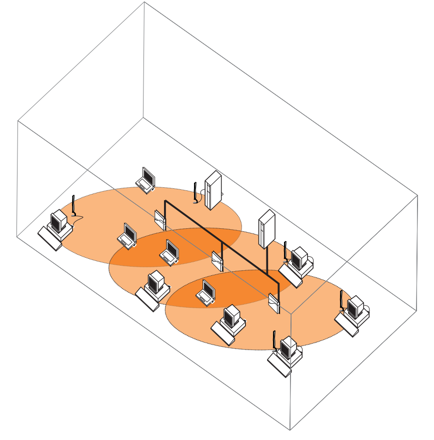
Die Beispiele auf den nächsten Seiten zeigen die Wirkung unterschiedlicher "Distance between APs"-Konfigurationen.

Abbildung 30 Parameter "Large Distance between APs" zeigt die Standardkonfiguration von Netzwerken; der Parameter **Distance between APs** wurde auf **Large** gesetzt.

- Aufgrund der Empfangsempfindlichkeit in diesem Modus, verzögert das drahtlose Gerät die Übertragung bei allen Telegrammen die sich in seinem Funkbereich befinden (farbige Kreise).
- Mobilen Stationen, die sich in einer bestimmten Zelle befinden, bleiben am versorgenden Access Point RLM angeschlossen, bis sie die drahtlose Zelle verlassen.

Diese Konfiguration bietet eine maximal mögliche Funkabdeckung bei geringster Anzahl an Radio Link Modules, die zur Abdeckung des drahtlosen Netzbereiches erforderlich sind.

Abbildung 30 Parameter "Large Distance between APs"



Die Beispiele in Abbildung 31 Parameter Medium Distance between APs und Abbildung 32 Parameter Small Distance between APs zeigen die Wirkung einer Änderung des Parameters Distance between APs. Obwohl die absolute Funkabdeckung gleich geblieben ist, wurde durch die Einstellung des Parameters Distance between APs die Abdeckung der drahtlosen Zelle aufgrund der unterschiedlichen Niveaus für die Empfangsempfindlichkeit in Wahrheit verringert:

- Die absolute Abdeckung der Access Points (RLMs) ist durch grau hinterlegte Kreise dargestellt
- Die verringerte Abdeckung ist durch farbige Bereiche dargestellt.

Durch die neue Konfiguration des Parameters Distance between APs, findet eine Verzögerung in den Stationen nur für Funksignale statt, die auf einem Pegel empfangen werden, der gleich oder höher dem Durchschnittspegel der farbigen Bereiche ist. Telegrammen mit einem niedrigeren Signalpegel werden als Verkehr einer anderen Zelle eingestuft und daher ignoriert, wenn die Station entscheidet, ob sie mit der Übertragung beginnen kann.

Mobile Stationen starten ihre Suche nach einem anderen RLM (bzw. verbinden sich) sobald sie den farbigen Bereich eines spezifischen Access Point RLM verlassen.

Abbildung 31 Parameter Medium Distance between APs

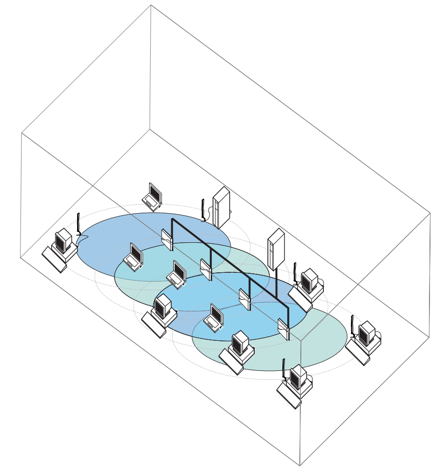
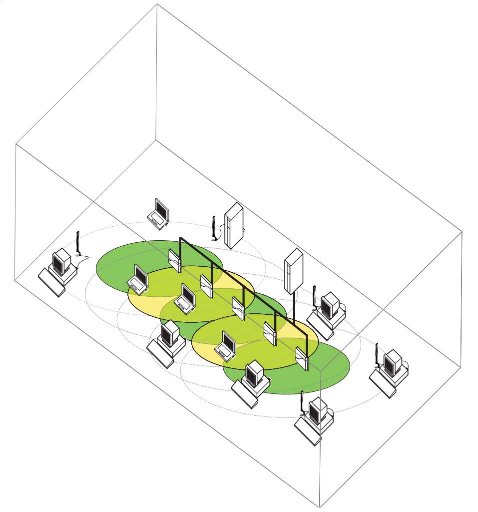


Abbildung 32 Parameter Small Distance between APs



7 Sicherheit

7.1 Einführung

Ein Vorteil des Standards IEEE 802.11 für drahtlose Netzwerke besteht darin, dass drahtlose Geräte einfach und schnell an ein Netzwerk angeschlossen werden können. Beispielsweise stellen drahtlose Stationen, die mit dem Netzwerknamen "ANY" konfiguriert wurden, eine Verbindung zum ersten IEEE 802.11-kompatiblen Access Point RLM her, das sie in Reichweite finden können.

Der Nachteil dieser "schnellen und einfachen Konnektivität" liegt in der Anfälligkeit des LAN gegenüber unberechtigten Zugriffen. Bedeutet dies, dass drahtlose LANs nicht sicher sind? Die Antwort lautet "Nein":

- Der Zugriff auf die Netzwerkressourcen wird über standardmäßige Sicherheitsmechanismen, wie beispielsweise Benutzernamen und Kennwörter, gesteuert.
- Mit Hilfe der Siemens SIMATIC NET IWL-Produkte können Sie zusätzliche Sicherheitsmaßnahmen zum Beschränken des Zugriffs auf Ihr drahtloses Gerät und/oder auf die Netzwerkressourcen anwenden.

In Abhängigkeit von der in Ihrer Netzwerkumgebung erforderlichen Sicherheitsstufe können diese Maßnahmen Folgendes umfassen:

- 7.2 Sichern des Zugriffs auf drahtlose Daten (Seite 172).
- 7.3 Drahtlose Datenverschlüsselung (Seite 186).
- 7.4 Sichern der Access Point RLM-Konfiguration (Seite 197).
- Erweiterte Sicherheitsmaßnahmen (Seite 204).

7.2 Sichern des Zugriffs auf drahtlose Daten

Damit unberechtigte Stationen nicht auf Daten zugreifen können, die über das Netzwerk übertragen werden, unterstützen die Produkte die folgenden Sicherheitsstufen:

- “Beschränken des drahtlosen Zugriffs auf das Netzwerk”
- Datenverschlüsselung zur Verschlüsselung aller über das drahtlose Gerät übertragenen Daten (siehe Drahtlose Datenverschlüsselung (Seite 186).

Diese Sicherheitsmaßnahmen finden Anwendung auf der "physikalischen Kommunikationsschicht" und ergänzen die "Benutzername/Kennwort"-Überprüfung auf der "Netzwerkschicht", die in den Standardnetzwerkbetriebssystemen implementiert ist.

7.2.1 Beschränken des drahtlosen Zugriffs auf das Netzwerk

Sie haben die folgenden Möglichkeiten, um zu verhindern, dass unbekannte und unberechtigte Datenverarbeitungsgeräte eine drahtlose Verbindung zum Netzwerk herstellen:

- Ausschließen all jener Stationen vom Netzwerk, die nicht mit dem korrekten Netzwerknamen konfiguriert wurden (siehe Sichern des drahtlosen Netzwerks (Seite 173).
- Verwenden von Zugriffskontrolltabellen, in denen die Stationen registriert werden, die zum Herstellen einer drahtlosen Verbindung zum Netzwerk berechtigt sind (siehe Zugriffskontrolle (Seite 176).

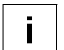
7.2.2 Sichern des drahtlosen Netzwerks

Durch das Sichern des drahtlosen Netzwerks wird verhindert, dass unberechtigte Benutzer auf das Access Point RLM in einem bestimmten SIMATIC NET IWL-Netzwerk Zugriff erhalten. Wenn ein Benutzer versucht, Zugriff auf das Netzwerk zu erhalten, seine Station jedoch nicht mit dem richtigen Netzwerknamen konfiguriert ist, dann ist die Station nicht in der Lage, das Bridging von Daten über das RLM auszuführen.

Es stehen zwei Optionen für diese Art der Zugriffssicherheit zur Verfügung: Die **offene** und die **geschlossene** Konfiguration.

- Die **offene** Konfiguration ist der IEEE 802.11-Standardmodus, der den folgenden Stationen den Zugriff auf das Access Point RLM gewährt:
  - Allen Stationen mit dem richtigen Netzwerknamen.
  - Allen Stationen, deren Netzwerkname auf "ANY" gesetzt ist.
- Die **geschlossene** Konfiguration ist der proprietäre SIMATIC NET IWL-Modus, der all jene Stationen von Ihrem Netzwerk ausschließt, die nicht mit dem richtigen Netzwerknamen konfiguriert sind.

  Diese Option verweigert den Zugriff auf folgende Stationen:
  - Alle SIMATIC NET IWL-Stationen, deren Netzwerkname auf "ANY" gesetzt ist, sowie
  - Alle Nicht-SIMATIC NET IWL-Stationen, deren Netzwerkname "zero string SSID" (Null-Netzwerkkennung) oder "ANY" lautet.



HINWEIS:

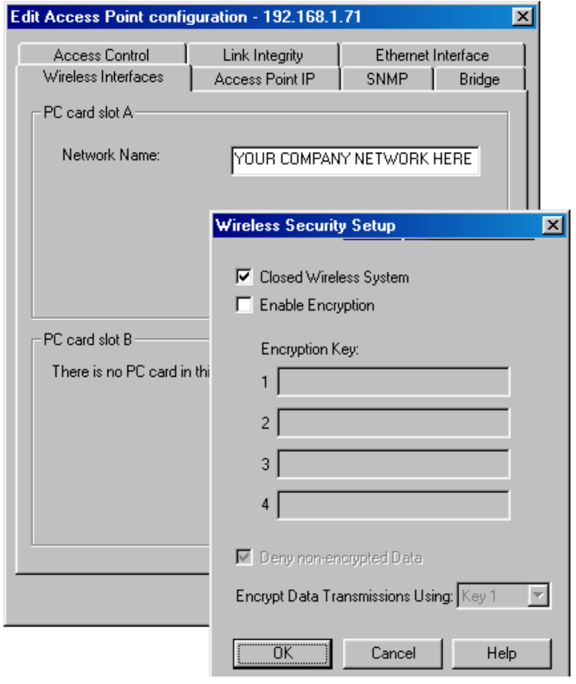
Die **geschlossene** Konfigurationsoption ist nicht mit dem IEEE 802.11-Standard für drahtlose LANs kompatibel.

Sichern des Zugriffs auf drahtlose Daten

Gehen Sie wie folgt vor, um Ihr Netzwerk zu sichern:

1. Starten Sie den RLM Manager, und wählen Sie das Access Point RLM.
2. Klicken Sie auf **Edit**, um eine Verbindung zum RLM herzustellen.
3. Wählen Sie die Registerkarte **Wireless Interfaces** (siehe Abbildung 33).
4. Wählen Sie die Schnittstelle (**PC Card slot A** oder **B**) des zu sichernden Netzwerks.
5. Klicken Sie auf die Schaltfläche **Security**, um die Sicherheitseigenschaften anzuzeigen.
6. Aktivieren Sie das Kontrollkästchen neben **Closed Wireless System**.
7. Klicken Sie zum Bestätigen auf **OK**, und schließen Sie das Fenster "Wireless Security Setup".

Abbildung 33 Sichern des drahtlosen Systems



8. (Optional) Klicken Sie auf die zweite Schnittstelle, um die Sicherheitsparameter festzulegen (kehren Sie zu Schritt 4 zurück).



ACHTUNG:
Das setzen von Parametern setzt den RLM zurück, es erfolgt ein Neuanlauf (reboot) und die Kommunikation zum und über den Accesspoint RLM ist für mindestens 15 Sekunden unterbrochen

9. Klicken Sie auf **OK**, um die neue Konfiguration auf dem Access Point RLM zu speichern und zum Hauptfenster von RLM Manager zurückzukehren.

Das Access Point RLM wird automatisch neu gestartet und beginnt den Bridging-Vorgang erneut, wobei nur Benutzern mit einem Netzwerknamen der Zugriff gewährt wird, der mit dem in der Konfiguration Ihrer Access Point RLMs festgelegten Namen übereinstimmt.

Wiederholen Sie die Schritte 1 bis 9 für alle weiteren Access Points (RLMs).

7.2.3 Zugriffskontrolle

Ein weiteres Verfahren zum Beschränken des drahtlosen Zugriffs auf das RLM (Radio Link-Modul) besteht in der Verwendung der Zugriffskontrolltabelle und/oder der Funktion für die RADIUS-Server-Zugriffskontrolle.

Wenn Sie die Funktion für die Zugriffskontrolle aktivieren, verhalten sich die RLMs wie folgt:

- Sie übertragen nur Telegramme an/von autorisierten Stationen, die in der Zugriffskontrolltabelle aufgeführt sind.

- Sie ignorieren alle Anforderungen zum Weiterleiten von Daten von/an nicht aufgeführte SIMATIC NET IWL-Stationen.

Die Aktivierung der Zugriffskontrolle ist ein rigoroserer Sicherheitsmechanismus als das “Sichern des drahtlosen Netzwerks”, da dieses Verfahren von den LAN-Administratoren verlangt, jeder einzelnen drahtlosen LAN-Station eine Berechtigung zu gewähren.

Um drahtlosen Stationen die Berechtigung für den Zugriff auf das Netzwerk zu gewähren, müssen die LAN-Administratoren Folgendes tun:

- Die eindeutige, universelle MAC-Adresse der drahtlosen LAN-Station in die Datei der Zugriffskontrolltabelle (*.tbl) einfügen.
- Die Datei der Zugriffskontrolltabelle auf alle RLMs laden.



HINWEIS:

Die Funktion für die Zugriffskontrolle ist in Netzwerkumgebungen, die lokale MAC-Adressen erfordern, nicht funktionsfähig.

Wenn Sie die RADIUS-Zugriffskontrolle aktivieren, können Sie Folgendes tun:

- Die Gültigkeitsdauer einer gewährten Berechtigung festlegen
- Das Berechtigungskennwort festlegen
- Maximal zwei RADIUS-Server für die Überprüfung der MAC-Adresse drahtloser Stationen zuweisen

Weitere Informationen zum Aktivieren der RADIUS-Server-Zugriffskontrolle finden Sie unter Aktivieren der RADIUS-Server-Zugriffskontrolle (Seite 183).

7.2.4 Aktivieren der Zugriffskontrolle

Wenn Sie die Zugriffskontrolle aktivieren möchten, müssen Sie zunächst mit Hilfe der Anwendung RLM Manager eine Zugriffskontrolltabellendatei (*.tbl) erstellen.

Sie können die Zugriffskontrolltabellendatei als Bestandteil einer (neuen) Konfiguration auf alle Radio Link-Module in Ihrem Netzwerk laden (weitere Informationen siehe Importieren einer Zugriffskontrolltabelle (Seite 181)).

7.2.5 Erstellen/Bearbeiten einer Zugriffskontrolltabelle

So erstellen oder bearbeiten Sie die Zugriffskontrolltabelle:

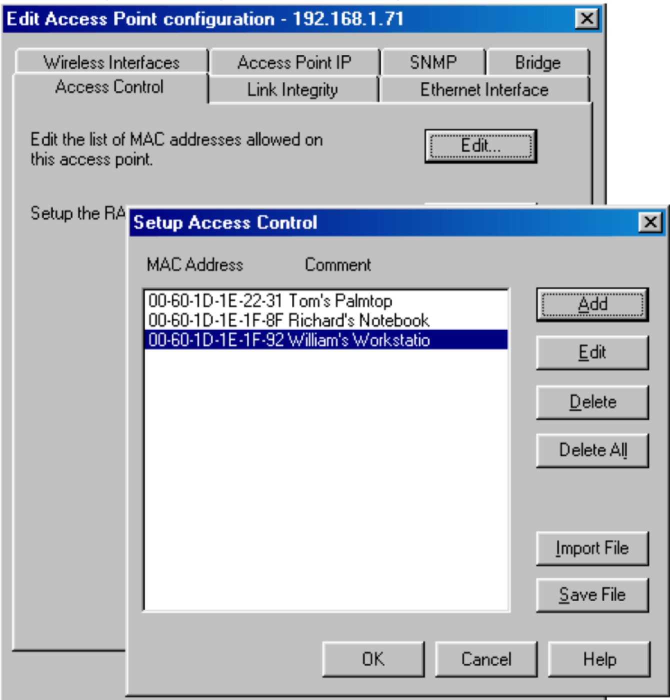
1. Starten Sie den RLM Manager, und wählen Sie das Radio Link-Modul.
2. Klicken Sie auf die Schaltfläche **Edit**.
3. Wählen Sie die Registerkarte **Access Control**.
4. Klicken Sie auf die Schaltfläche **Edit**, um alle derzeit autorisierten MAC-Adressen, wie in Abbildung 34 Konfigurieren der Zugriffskontrolle ersichtlich, anzuzeigen.

   Die Zugriffskontrolle ist standardmäßig auf **<All will be permitted>** eingestellt, d.h., es sind gegenwärtig keine Zugriffsbeschränkungen definiert.
5. Ändern Sie die Tabelle der MAC-Adressen anhand der folgenden Schaltflächen:

- **Add** - Zum Hinzufügen von jeweils einer neuen MAC-Adresse. Sie können auch einen Namen im Feld **Comments** eingeben oder eine Anmerkung zur aufgeführten MAC-Adresse einfügen.
- **Edit** - Zum Ändern von Einträgen in der Tabelle.
- **Delete** - Zum Entfernen von jeweils einer MAC-Adresse.
- **Delete All** - Zum Entfernen aller MAC-Adressen und zum Deaktivieren der Zugriffskontrolle.
- **Import File** - Zum Importieren einer vorhandenen Zugriffskontrolltabelle.
- **Save File** - Zum Speichern der derzeitigen Zugriffskontrolltabelle in einer Datei.

6. Wiederholen Sie den Schritt 5 für alle Stationen, denen Sie eine Berechtigung für das Senden/Empfangen von Daten über dieses RLM gewähren möchten.

Abbildung 34 Konfigurieren der Zugriffskontrolle



7. Klicken Sie auf die Schaltfläche **Save file**, um eine Sicherungskopie der gerade erstellten Zugriffskontrolltabellendatei (*.tbl) zu erstellen.

   Sie können diese Datei später zum Importieren der Konfiguration auf ein anderes Access Point RLM verwenden.
8. Klicken Sie auf **OK**, um zur Registerkarte "Access Control" zurückzukehren.
9. Klicken Sie erneut auf **OK**, um die neue Konfiguration auf dem RLM zu speichern und zum Hauptfenster von RLM Manager zurückzukehren.
10. (Optional) Speichern Sie die Konfiguration, wie in Schritt 4 - Erstellen einer Sicherungsdatei der Konfiguration (Seite 72) beschrieben, als lokale Sicherungsdatei (*.cnf).

Weitere Informationen zum Speichern der Tabelle auf allen RLMs finden Sie unter Importieren einer Zugriffskontrolltabelle (Seite 181)[1].

7.2.6 Importieren einer Zugriffskontrolltabelle

So importieren Sie eine Zugriffskontrolltabellendatei (*.tbl) in Ihre Radio Link-Module:

1. Starten Sie den RLM Manager, und stellen Sie eine Verbindung zum Access Point RLM im Bearbeitungsmodus her.
2. Wählen Sie die Registerkarte **Access Control**, und klicken Sie auf die Schaltfläche **Edit**, um alle derzeit berechtigten MAC-Adressen anzuzeigen.
3. Klicken Sie auf die Schaltfläche **Import File**, und wählen Sie die zu importierende Zugriffskontrolltabellendatei (*.tbl) aus.

1. Weitere Informationen finden Sie außerdem unter 8.3.1 Allgemeine Parameter (Seite 243).

4. Klicken Sie auf die Schaltfläche **Öffnen**, um die ausgewählte Datei zu importieren.
5. Klicken Sie auf **OK**, um zur Registerkarte **Access Control** zurückzukehren.
6. Klicken Sie erneut auf **OK**, um die neue Konfiguration auf dem Radio Link-Modul zu speichern und zum Hauptfenster von RLM Manager zurückzukehren.
7. (Optional) Speichern Sie die Konfiguration, wie in Schritt 4 - Erstellen einer Sicherungsdatei der Konfiguration (Seite 72) beschrieben, als lokale Sicherungsdatei (*.cnf).

7.2.7 Deaktivieren der Zugriffskontrolle

So deaktivieren Sie die Zugriffskontrolle für Ihre Radio Link-Module:

1. Starten Sie den RLM Manager, und stellen Sie eine Verbindung zum Radio Link-Modul im Bearbeitungsmodus her.
2. Wählen Sie die Registerkarte **Access Control**, und klicken Sie auf die Schaltfläche **Edit**, um alle derzeit autorisierten MAC-Adressen anzuzeigen.
3. Klicken Sie zum Deaktivieren der Zugriffskontrolle auf die Schaltfläche **Delete All**. Im Fenster "MAC address" erscheint nun die Angabe **<All will be permitted>**.
4. Klicken Sie auf **OK**, um zur Registerkarte **Access Control** zurückzukehren.
5. Klicken Sie erneut auf **OK**, um die neue Konfiguration auf dem RLM zu speichern und zum Hauptfenster von RLM Manager zurückzukehren.

6. (Optional) Speichern Sie die Konfiguration, wie in Schritt 4 - Erstellen einer Sicherungsdatei der Konfiguration (Seite 72) beschrieben, als lokale Sicherungsdatei (*.cnf).
7. Aktualisieren Sie das Formular "Access Point Configuration Record", um diese Änderung festzuhalten.
8. (Optional) Ändern Sie die Zugriffskontrolleinstellungen für alle anderen Radio Link-Module.

7.2.8 Aktivieren der RADIUS-Server-Zugriffskontrolle

Die RADIUS-Server-Zugriffskontrolle ist ein Verfahren, bei dem Radio Link-Module in Verbindung mit einem RADIUS-Server eines Fremdanbieters verwendet werden.

Um die RADIUS-Server-Zugriffskontrolle verwenden zu können, müssen Sie Folgendes tun:

1. Einen RADIUS-Server einrichten.

2. Den RADIUS-Server wie folgt konfigurieren:
   - Die Liste der MAC-Adressen muss zusammen mit dem Kennwort (=Berechtigungskennwort) in die Datei/Datenbank "users" des Servers eingegeben werden.

- Außerdem muss eine Liste der IP-Adressen aller Radio Link-Module erstellt werden, die den RADIUS-Server verwenden werden. Diese Liste muss zusammen mit dem Berechtigungskennwort in die Datei/Datenbank "station" des Servers eingegeben werden.

3. Eine Liste der MAC-Adressen aller (drahtlosen) Stationen erstellen, die Sie für das Herstellen einer drahtlosen Verbindung mit Ihrer RLM-Infrastruktur berechtigen möchten.
4. Die Radio Link-Module wie folgt konfigurieren:
   - Die Authenfizierung von RADIUS-MAC-Adressen aktivieren
   - Die Gültigkeitsdauer der RADIUS-Berechtigung festlegen
   - Das Berechtigungskennwort festlegen
   - Die IP-Adresse des RADIUS-Servers angeben
   - Den Authentifizierungsport des RADIUS-Servers angeben

7.2.8.1 RADIUS-Server-Zugriffskontrolle

Mit Hilfe der RADIUS-Zugriffskontrolle können Sie Folgendes tun:

- Die Gültigkeitsdauer einer gewährten Berechtigung festlegen
- Das Berechtigungskennwort festlegen
- Maximal zwei RADIUS-Server für die Überprüfung der MAC-Adresse drahtloser Stationen zuweisen

Für jeden RADIUS-Server müssen Sie Folgendes angeben:

- Die eindeutige IP-Adresse des RADIUS-Servers
- Den vom ausgewählten Server verwendeten Authentifizierungsport.

So beschränken Sie den Zugriff auf Ihr Netzwerk mit Hilfe der Zugriffskontrolle für MAC-Adressen auf einem RADIUS-Server:

1. Starten Sie den RLM Manager, und wählen Sie das Access Point RLM.
2. Klicken Sie auf die Schaltfläche **Edit**.
3. Wählen Sie die Registerkarte **Access Control**.
4. Klicken Sie auf die Schaltfläche **RADIUS Server** im unteren Bereich der Registerkarte, um den RADIUS-Servernamen und den versteckten Parameter anzuzeigen.
5. Aktivieren Sie das Kontrollkästchen **Enable RADIUS Server**.
   - Der Standardwert ist: RADIUS Access Control Disabled

Weitere Informationen finden Sie in der Hilfedatei (drücken Sie die Funktionstaste F1 von RLM Manager.

7.3 Drahtlose Datenverschlüsselung

Um die höchste Sicherheitsstufe für die Übertragung von drahtlosen Daten über Ihr Netzwerk zu gewährleisten, können Sie die WEP-Datenverschlüsselung (Wired Equivalent Privacy, WEP) nutzen.

Um die WEP-Datenverschlüsselung in Ihrem Netzwerk verwenden zu können, müssen Sie folgende Voraussetzungen erfüllen:

- Alle drahtlosen Stationen und Access Points müssen mit CP 1515-Karten ausgerüstet sein.
- Alle Geräte müssen mit übereinstimmenden Werten für die WEP-Chiffrierschlüssel konfiguriert sein.

Bei der WEP-Datenverschlüsselung werden Chiffrierschlüssel mit 13 Zeichen auf der Basis des RC4-Verschlüsselungsalgorithmus verwendet, der zum Verschlüsseln/Entschlüsseln aller über die drahtlose Schnittstelle übertragenen Daten verwendet wird.

Sie können bis zu 4 unterschiedliche Schlüssel zum **Entschlüsseln** drahtloser Daten angeben und einen der angegebenen Dechiffrierschlüsselwerte zum **Verschlüsseln** drahtloser Daten auswählen.

Da 4 unterschiedliche Schlüssel zum Entschlüsseln drahtloser Daten verfügbar sind, können Sie Ihre WEP-Schlüssel in regelmäßigen Zeitabständen wechseln, ohne dass sich dies auf die normale Netzwerkleistung auswirkt (siehe auch Verwalten von WEP-Chiffrierschlüsseln (Seite 204).

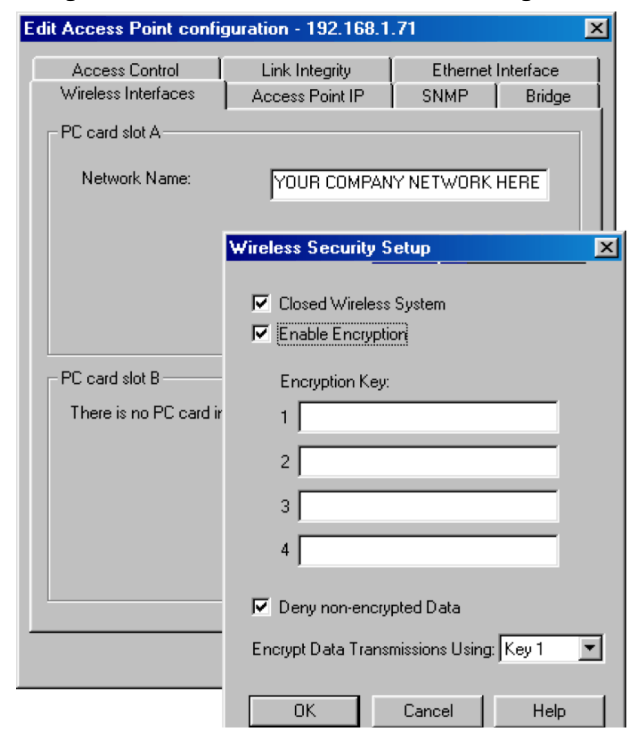
7.3.1 Aktivieren der WEP-Verschlüsselung

Damit Sie die WEB-Verschlüsselung aktivieren können, müssen Sie Folgendes sicherstellen:

- Dass alle drahtlosen Geräte mit CP 1515-Karten ausgerüstet wurden.
- Dass alle drahtlosen Geräte mit übereinstimmenden Chiffrierschlüsselwerten konfiguriert sind.

Es empfiehlt sich, die vorgeschlagenen WEP-Schlüsselwerte im Radio Link-Modul-Konfigurationsprotokoll zu notieren und an einem sicheren Ort zu verwahren.

Abbildung 35 Aktivieren der WEP-Verschlüsselung



Anhand der WEP-Datenverschlüsselung (Wired Equivalent Privacy, WEP) können Sie alle Daten verschlüsseln, die über das drahtlose LAN-Medium übertragen werden.

Damit Sie WEP in Ihrem Netzwerk verwenden können, müssen alle Access Points und drahtlosen Stationen mit CP 1515-Karten ausgerüstet sein, die für die Verwendung identischer Chiffrierschlüssel konfiguriert sind.

So aktivieren Sie die Verschlüsselung:

1. Starten Sie den RLM Manager, und wählen Sie das RLM.
2. Klicken Sie auf die Schaltfläche **Edit**.
3. Wählen Sie die Registerkarte **Wireless Interfaces** .
4. Klicken Sie auf die Schaltfläche **Security** , um das Fenster "Wireless Security Setup" anzuzeigen (siehe Abbildung 35 Aktivieren der WEP-Verschlüsselung).
5. Aktivieren Sie das Kontrollkästchen **Enable Encryption**, um die Verschlüsselung zu aktivieren, und:
   - Geben Sie bis zu 4 verschiedene Schlüssel zum Entschlüsseln von Daten ein, die über die drahtlose Schnittstelle empfangen wurden.
   - Wählen Sie einen dieser Schlüssel zum Verschlüsseln drahtloser Daten aus, die über die drahtlose Schnittstelle übertragen werden sollen.
6. Klicken Sie auf **OK**, um zur Registerkarte **Wireless Interfaces** zurückzukehren.

7. Klicken Sie erneut auf **OK**, um die Konfiguration auf dem Radio Link-Modul zu speichern und zum Hauptfenster von RLM Manager zurückzukehren.
   Das RLM wird nun neu gestartet.

Optional können Sie das Access Point RLM so konfigurieren, dass die Übertragung nicht verschlüsselter Daten zugelassen oder verweigert wird.

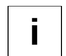
7.3.1.1 WEP-Chiffrierschlüsselwerte

Wenn Sie die Verschlüsselung aktivieren, haben Sie die Möglichkeit zur Eingabe der folgenden Chiffrierschlüssel.

Für die CP 1515-Karte, die den 128-Bit-RC4-Verschlüsselungsalgorithmus unterstützt, sind folgende Werte gültig:

- Alphanumerischer Werte mit 13 Zeichen im Bereich von "a-z" und "0-9"
  Beispiel: SECURE1234567
- Hexadezimalwerte mit 26 Zeichen, denen die Zeichen "0x" (Null x) voranstehen.
  Beispiel: 0x1234567890ABCDEF1234567890
- Optional können Sie auch Kurzwerte (beispielsweise 64-Bit-Werte) verwenden

Hexadezimalzeichenfolgen, denen kein "0x" voransteht, werden als alphanumerische Zeichenfolgen interpretiert.



HINWEIS:

Die von Ihnen eingegebenen WEP-Schlüsselwerte sind nur sichtbar, während Sie die Zeichenfolgen eingeben. Sobald Sie das Fenster

"Security Setup" schließen, werden die Werte als verborgene Zeichen gespeichert: d.h., beim nächsten Öffnen des Fensters "Security Setup" sind die WEP-Schlüsselwerte nicht mehr sichtbar. Es empfiehlt sich, die eingegebenen Werte vor dem Schließen des Fensters zu notieren.

7.3.1.2 WEP-Übertragungsschlüsselwert

Wenn Sie die WEP-Verschlüsselung aktivieren, können Sie einen Schlüssel für die Übertragung drahtloser Daten in der Liste der WEP-Chiffrierschlüsselwerte auswählen. Sie können nur einen Übertragungsschlüssel auswählen, dem ein korrekter WEP-Chiffrierschlüsselwert zugewiesen ist. Falls Sie nicht mehr als 2 Schlüsselwerte angegeben haben, können Sie den Übertragungsschlüssel nur aus diesen beiden Werten wählen.



ACHTUNG:
Falls Sie das Kontrollkästchen "Deny non-encrypted Data" deaktiviert haben, überträgt das RLM auch im "Nicht-Verschlüsselungsmodus".

7.3.1.3 Abweisen nicht verschlüsselter Daten

Wenn Sie die WEP-Verschlüsselung für drahtlose Daten verwenden möchten, sollten Sie alle Daten verschlüsseln, die über das drahtlose Medium übertragen werden.

In einigen Fällen können Sie jedoch zulassen, dass das Radio Link-Modul auch nicht verschlüsselte Daten verarbeitet.

Im Folgenden finden Sie Beispiele für solche Situationen:

- Netzwerkumgebungen, die sowohl drahtlose Stationen mit Karten (CP 1515), die die WEP-Verschlüsselung unterstützen, als auch Karten umfassen, die keine Verschlüsselung unterstützen.
- Netzwerkumgebungen, in denen Sie eine große Anzahl drahtloser Stationen mit werkseitig eingestellter Konfiguration installieren möchten, für die die Verschlüsselung standardmäßig deaktiviert ist.

Wenn Sie solche Stationen mit der werkseitigen Standardkonfiguration starten, wären diese Stationen nicht in der Lage, eine Verbindung zum Netzwerk herzustellen, da sie die verschlüsselten Telegramme nicht interpretieren könnten.

Um einen optimalen Schutz vor unberechtigten Zugriffen auf Ihr Netzwerk zu gewährleisten, sollten Sie die Option **Deny non-encrypted data** immer aktiviert lassen (=Standard).



ACHTUNG:
Sie sollten dieses Kontrollkästchen nur dann deaktivieren, wenn hierfür gute Gründe vorliegen. Beispielsweise, um es dem RLM zu erlauben, mit drahtlosen Stationen zu kommunizieren, die mit und ohne WEP-Verschlüsselung arbeiten, oder die WEP-Verschlüsselung zu aktivieren oder zu deaktivieren.
Lesen Sie den folgenden Abschnitt, bevor Sie das Kontrollkästchen Deny non-encrypted Data deaktivieren.

7.3.1.4 Funktionsweise der WEP-Verschlüsselung

Der IEEE 802.11-Standard für drahtlose LANs wurde entwickelt, um benutzerfreundliche und einfach installierbare drahtlose Netzwerke realisieren zu können, die es den Benutzern erlauben, drahtlose LAN-Produkte verschiedener Anbieter zusammen zu nutzen.

Der Nachteil des einfachen Zugriffs und der Interoperabilität besteht in der Anfälligkeit gegenüber unberechtigten Zugriffen und/oder der unberechtigten Nutzung Ihres Netzwerks. Die WEP-Verschlüsselung stellt zwar eine gute Möglichkeit zum Sichern des Zugriffs auf Ihre drahtlosen Daten dar, jedoch sollten Sie einige Dinge berücksichtigen, um sicherzustellen, dass Ihr Netzwerk die richtige Sicherheitsstufe aufweist.

Wenn Sie die WEP-Verschlüsselung aktivieren, stehen zwei WEP-Betriebsmodi zur Verfügung:

- Aktivieren der Verschlüsselung und Abweisen nicht verschlüsselter Daten
- Aktivieren der Verschlüsselung und Zulassen nicht verschlüsselter Daten

Um einen optimalen Schutz zu gewährleisten, sollten Sie die Option **Deny non-encrypted data** immer aktiviert lassen (=Standard).

7.3.1.5 Aktivieren der Verschlüsselung und Abweisen nicht verschlüsselter Daten

Wenn Sie die Option zum Aktivieren der Verschlüsselung und Abweisen nicht verschlüsselter Daten aktivieren, verhält sich das Radio Link-Modul wie folgt:

Drahtlose Datenverschlüsselung

- Es verarbeitet an der drahtlosen Schnittstelle empfangene Telegramme nur, wenn die Telegramme anhand eines der vier angegebenen Schlüssel verschlüsselt wurden.
- Es überträgt drahtlose Daten immer mit Hilfe des ausgewählten WEP-Schlüssels.
- Es verschlüsselt außerdem den gesamten Multicast- und Broadcast-Verkehr, den es an das drahtlose Medium überträgt.

Wenn Ihr Netzwerk drahtlose Stationen ohne übereinstimmenden WEP-Schlüssel bzw. drahtlose Stationen mit PC-Karten enthält, die die WEP-Verschlüsselung nicht unterstützen, können diese Stationen keine drahtlose Verbindung herstellen, da sie wesentliche Netzwerkinformationen nicht "verstehen" (entschlüsseln) können.

7.3.1.6 Aktivieren der Verschlüsselung und Zulassen nicht verschlüsselter Daten

Wenn Sie die Option zum Aktivieren der Verschlüsselung aktiviert, jedoch das Kontrollkästchen **Deny non-encrypted data** deaktiviert haben, verhält sich das RLM wie folgt:

- Es verarbeitet alle an der drahtlosen Schnittstelle empfangenen Telegramme, unabhängig davon, ob die Telegramme anhand eines der vier angegebenen Schlüssel verschlüsselt wurden oder nicht.
- Es verschlüsselt drahtlose Daten auf der Grundlage der Verschlüsselungseinstellungen der Empfängerstation.
- Wenn die Empfängerstation die WEP-Verschlüsselung verwendet, sendet das Radio Link-Modul die Telegramme anhand des ausgewählten Übertragungsschlüsselwertes im verschlüsselten Format.

- Wenn die Empfängerstation keine WEP-Verschlüsselung verwendet, sendet das Acess Point RLM die Meldung im nicht verschlüsselten Format.
- Wenn die Datenmeldung eine Multicast- oder Broadcast-Telegramm ist, die in der Regel an "alle Stationen" adressiert ist, sendet das Radio Link-Modul dieses Telegramm im nicht verschlüsselten Format.

Das Verhalten des Radio Link-Moduls steht in keiner Beziehung zu der Art und Weise, wie die drahtlose Meldung vom RLM empfangen wurde. Wenn eine drahtlose Station, die die WEP-Verschlüsselung verwendet, beispielsweise Daten an eine Station in der gleichen drahtlosen Zelle senden möchte, erfolgt die Übertragung folgendermaßen:

- Verschlüsselte Übertragung von der WEP-Station zum RLM
- Nicht verschlüsselte Übertragung vom Radio Link-Modul an das Ziel, wenn die Empfängerstation keine WEP-Verschlüsselung unterstützt oder die WEP-Option nicht aktiviert hat.



ACHTUNG:
Für die meisten Netzwerkumgebungen, die eine höhere Sicherheitsstufe als die von SIMATIC NET IWL und von den meisten der heutigen Netzwerkbetriebssysteme (z.B. Benutzernamen und Kennwörter) unterstützten standardmäßigen Sicherheitsmechanismen erfordern, empfiehlt Siemens, diese Option nicht zu verwenden, es sei denn, Sie möchten Client-Stationen jeder Art einfachen Zugriff gewähren und/oder die Migration ist für Ihr Datennetzwerk wichtiger als eine hohe Sicherheitsstufe.

7.3.1.7 Hinweise zur Verwaltung von Chiffrierschlüsseln

Die WEP-Verschlüsselung ist, ähnlich wie andere Eigenschaften, so sicher wie das Türschloss eines Hauses: d.h., wenn Sie keine Sicherheitsrichtlinien auf die Personen anwenden, die zur Verwendung des Schlüssels berechtigt sind, oder die wissen, wo dieser Schlüssel zu finden ist, kann sogar das sicherste Schloss von einem Eindringling geöffnet werden.

Deshalb würden Sie den Schlüssel zu Ihrem Haus auch nicht unter dem Fußabtreter vor der Tür "verstecken". Ähnliche Sicherheitsrichtlinien sollten auch auf die zum Verschlüsseln der drahtlosen Kommunikation verwendeten Schlüssel angewendet werden.

Um das Risiko eines Bekanntwerdens der WEP-Schlüsselwerte gegenüber Unberechtigten zu minimieren, empfehlen sich die folgenden Maßnahmen:

- Halten Sie alle Registrierungsunterlagen, auf denen die WEP-Schlüsselwerte verzeichnet/definiert sind, unter Verschluss.
- Ändern Sie die WEP-Chiffrierschlüsselwerte in regelmäßigen Zeitabständen sowohl auf den Stationen als auch auf den RLMs.

Die Möglichkeit, bis zu 4 verschiedene Schlüssel zum Entschlüsseln von Daten einzugeben, die über die drahtlose Schnittstelle empfangen werden, erlaubt es Ihnen, ein WEP-Schlüsselrotationsschema zu definieren.

Sie können beispielsweise alle x Wochen einen neuen Übertragungsschlüssel auswählen, bis der vierte an der Reihe ist. Zu diesem Zeitpunkt könnten Sie 3 neue WEP-Schlüsselwerte für die ersten drei WEP-Schlüsseleinträge eingeben, bevor die Gültigkeit des vierten Schlüsselwerts abgelaufen ist. Sobald alle Stationen und Radio Link-Module für die Verwendung des ersten neuen Schlüssels konfiguriert sind, können Sie den vierten Schlüsselwert durch einen neuen WEP-Schlüsselwert ersetzen.

7.4 Sichern der Access Point RLM-Konfiguration

Sicherheitsmaßnahmen, wie die Zugriffskontrolle, verlieren ihre Wirksamkeit, wenn unberechtigte Personen die Konfiguration Ihrer Radio Link-Module anzeigen und ändern können.

Um die Netzwerkkonfiguration vor unerwünschten Änderungen zu schützen, empfiehlt sich die Implementierung der folgenden Maßnahmen:

- Kennwörter für Lese- und Lese-/Schreibvorgänge
- Zugriffsliste für SNMP-IP-Adressen
- Trap Host-Benachrichtigungsmechanismen (optional)

7.4.1 Kennwörter für Lese- und Lese-/ Schreibvorgänge

Um den Zugriff auf die Access Point RLM-Konfigurationsinformationen zu beschränken, können Sie zwei Zugriffsebenen für Kennwörter festlegen:

- Kennwort für Lesevorgänge
- Kennwort für Lese-/Schreibvorgänge

7.4.1.1 Kennwort für Lesevorgänge

Das Kennwort für Lesevorgänge gewährt den Zugriff auf das Radio Link-Modul nur für die Überwachung von Diagnoseinformationen, die nach Auswahl der Schaltfläche **Monitor** im Hauptfenster von RLM Manager angezeigt werden.

Sie können das Kennwort für Lesevorgänge im Feld **Read Password** auf der Registerkarte **SNMP** definieren. (Wählen Sie das Access Point RLM in der Liste aus, klicken Sie auf **Edit**, und wählen Sie die Registerkarte **SNMP**.) Der Standardwert ist "public".

7.4.1.2 Kennwort für Lese-/Schreibvorgänge

Das Kennwort für Lese-/Schreibvorgänge gewährt Ihnen vollen Zugriff auf die RLM-Diagnoseinformationen, die nach Auswahl der Schaltfläche **Monitor** angezeigt werden, sowie auf die Konfigurationseinstellungen, die nach Auswahl der Schaltfläche **Edit** erscheinen.

Die Eingabe eines falschen Kennworts führt zu einem Zeitüberschreitungsfehler oder zu einer Fehlermeldung wie etwa "SNMP error no such name".

So definieren Sie ein Kennwort für Lese-/Schreibvorgänge:

1. Starten Sie den RLM Manager, und wählen Sie das Ziel-RLM in der Liste aus, oder geben Sie eine bestimmte IP-Adresse ein.
2. Klicken Sie auf die Schaltfläche **Edit**, um eine Verbindung zum Radio Link-Modul herzustellen.
3. Wählen Sie die Registerkarte **SNMP**.
4. Geben Sie im Feld **Read/Write Password** das neue Kennwort ein. Der Standardwert ist "public".
5. Klicken Sie auf **OK**, um die Konfiguration auf dem Radio Link-Modul zu speichern. Das RLM wird nun neu gestartet.

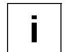
7.4.2 SNMP-IP-Zugriffsliste

Neben der Beschränkung durch Kennwörter für Lese- und Lese-/Schreibvorgänge können Sie den Zugriff auf die RLM-Konfiguration auch auf eine bestimmte Zahl autorisierter Stationen beschränken.

Um der SIMATIC NET IWL-Verwaltungsstation die Berechtigung für den Zugriff auf Ihre Radio Link-Module zu gewähren, müssen Sie Folgendes angeben:

- Die eindeutige IP-Adresse der Verwaltungsstation, und
- Die RLM-Schnittstelle (Port), über die diese Station auf die Konfiguration zugreift

Wenn Sie mehrere Stationen autorisieren möchten, können Sie einen Bereich von IP-Adressen angeben, den Sie für autorisierte LAN-Administratorstationen reservieren.



HINWEIS:

Wenn Sie die SNMP-IP-Zugriffsliste verwenden, sollten Sie die IP-Adressen aller Stationen einfügen, die Konfigurations- oder Diagnoseinformationen vom Radio Link-Modul abrufen müssen, d.h., Stationen von Administratoren, die entweder Kennwörter für Lesevorgänge oder für Lese-/Schreibvorgänge verwenden.

Wenn die IP-Adresse oder Schnittstelle nicht mit dem Eintrag in der SNMP-IP-Zugriffsliste übereinstimmt, wird dem Absender der Anforderung ein Zeitüberschreitungsfehler angezeigt.

So gewähren Sie einer Verwaltungsstation die Berechtigung über die SNMP-IP-Zugriffsliste:

1. Starten Sie den RLM Manager, und wählen Sie das Access Point RLM.
2. Klicken Sie auf die Schaltfläche **Edit**, um eine Verbindung zum Radio Link-Modul herzustellen.
3. Wählen Sie die Registerkarte **SNMP**, um die SNMP-Parameter anzuzeigen. Die **SNMP-IP-Zugriffsliste** erscheint unten auf der Registerkarte **SNMP**, wie in SNMP-Parameter einrichten (Seite 235) ersichtlich.
4. Ändern Sie die SNMP-IP-Zugriffsliste mit Hilfe der folgenden Schaltflächen:
   - **Add** - Zum Hinzufügen von IP-Adressen zur Liste. (Drücken Sie die Taste F1, um Online-Hilfe zu möglichen Werten für diese Felder zu erhalten.)
   - **Delete** - Zum Entfernen von IP-Adressen aus der Liste.
   - **Edit** - Zum Ändern von Einträgen in der Liste.

   Der Standardwert ist **<All will be permitted>**.

7.4.3 Trap Host-Nachrichten

Über den Trap Host-Mechanismus können Sie den Netzwerkadministrator informieren, wenn das Radio Link-Modul zurückgesetzt bzw. ein erzwungener Neustart ausgeführt wird, oder wenn ein Authentifizierungsfehler auftritt bzw. eine aktive oder unterbrochene Verbindung festgestellt wird. Die Trap Host-Nachricht erlaubt es dem

Administrator, festzustellen, ob der Zurücksetzungsvorgang oder der erzwungene Neustart eine berechtigte Aktion war.

7.4.3.1 Aktivieren von Trap Host-Nachrichten

So aktivieren Sie den Trap Host-Mechanismus:

1. Starten Sie den RLM Manager, und wählen Sie das Radio Link-Modul.
2. Klicken Sie auf die Schaltfläche **Edit**, um eine Verbindung zum RLM herzustellen.
3. Wählen Sie die Registerkarte **SNMP**, um die SNMP-Parameter anzuzeigen.
4. Geben Sie im Feld **Trap Host IP Address** Folgendes ein:
   - **Eine beliebige gültige IP-Adresse** - An diese IP-Adresse wird eine Meldung gesendet, wenn das Radio Link-Modul zurückgesetzt wird.
   - **0.0.0.0 - (Anfangswert)** - Zum Deaktivieren des SNMP-Trap-Agenten.
5. Geben Sie ein Kennwort im Feld **Trap Host Password** ein.

   Wählen Sie ein Kennwort, das mit dem auf dem Trap Host festgelegten Kennwort übereinstimmt, um unerwünschte oder unberechtigte SNMP-Trap-Nachrichten auf dem Trap Host zu filtern.

   Das Trap Host-IP-Kennwort wird in die SNMP-Trap-Nachrichten eingebettet, die von diesem RLM gesendet werden. Wenn der Trap Host eine Nachricht ohne Kennwort bzw. mit unbekanntem Kennwort empfängt, wird die Trap-Nachricht ignoriert.

  - **Gültige Werte**: Ein beliebiger alphanumerischer Wert im Bereich von a-z und 0-9 mit mindestens 2 und maximal 31 Zeichen.
  - **Anfangswert**: public

6. Klicken Sie auf **OK**, um die neue Konfiguration auf dem Access Point RLM zu speichern und zum Hauptfenster von RLM Manager zurückzukehren.

Wenn Sie die Trap Host-Nachrichten aktivieren, sollten Sie Folgendes berücksichtigen:

- Die IP-Adresse muss die Trap Host-Station kennzeichnen, d.h. die Netzwerkverwaltungsstation, die für den Empfang der Trap-Nachrichten verwendet wird.
- Das Trap Host-Kennwort wird in die Trap-Nachrichten eingefügt. Anhand dieses Kennworts kann die Trap Host-Station feststellen, ob eine Trap Host-Nachricht aus ihrer eigenen Domäne stammt oder nicht.

7.4.3.2 Trap Host:Nachrichten

Folgende Meldungstypen werden unterschieden:

- "Call Boot"-Trap-Nachrichten
- Authentifizierungsfehlermeldungen
- Meldungen über aktive oder unterbrochene Verbindungen

7.4.3.3 "Call Boot"-Trap-Nachrichten

"Call Boot"-Trap-Nachrichten kommen in den folgenden Situationen vor:

- Beim Zurücksetzen eines Radio Link-Moduls
- Bei Stromausfall

- Bei Änderungen der RLM-Konfiguration

7.4.3.4 Authentifizierungsfehlermeldungen

Dieser Meldungstyp wird an die LAN-Administratorstation gesendet, wenn ein falsches Kennwort auf einer (mobilen) Station eingegeben wurde. Das Radio Link-Modul reagiert jedoch nicht, und es kommt zu einem Zeitüberschreitungsfehler.

7.4.3.5 Meldungen über aktive oder unterbrochene Verbindungen

Dieser Meldungstyp kann für die Benachrichtigung über Probleme mit der Verbindungsintegrität verwendet werden. Wenn beispielsweise, bei einer doppelten Ethernetverbindung (siehe auch Kapitel 6.2.9 Link Integrity (Seite 160)), eine Ethernetverbindung unterbrochen wird, dann wird eine Trap-Nachricht über eine unterbrochene Verbindung ("link down") gesendet. Aufgrund dieser Nachricht wird die andere Ethernetverbindung verwendet. Sobald die Verbindung (die ursprüngliche Verbindung) wiederhergestellt ist, wird eine Meldung über eine aktive Verbindung ("link up") generiert. Die ursprüngliche Verbindung kann wieder verwendet werden.

7.5 Erweiterte Sicherheitsmaßnahmen

7.5.1 Verwalten von Zugriffskontrolltabellen

Es empfiehlt sich, eine zentrale Zugriffskontrolltabelle zu erstellen und auf der Festplatte der LAN-Administratorstation zu speichern und/oder für andere LAN-Administratorstationen freizugeben. Darüber hinaus sollten Sie nur eine Tabelle für alle Radio Link-Module verwenden.

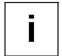
Weitere Informationen finden Sie unter Erstellen/Bearbeiten einer Zugriffskontrolltabelle (Seite 178).

7.5.2 Verwalten von WEP-Chiffrierschlüsseln

Die WEP-Verschlüsselungsfunktion erlaubt es dem drahtlosen System, bis zu vier verschiedene Schlüssel gleichzeitig zu unterstützen. Dies entspricht dem 802.11-Standard, der vier so genannte "Standardschlüssel" vorschreibt.

Mit Hilfe dieser Schlüssel kann der Übergang von der Verwendung eines Schlüssels zur Verwendung des nächsten Schlüssels nahtlos erfolgen. Die allgemeine Voraussetzung dafür, dass eine verschlüsselte Übertragung zwischen zwei Karten erfolgen kann, besteht im Vorhandensein eines gemeinsamen Schlüsselwertes mit der gleichen Schlüsselindexnummer im Bereich der vier Schlüssel zum Zeitpunkt der Übertragung. Der Schlüsselindex des Schlüssels, der zur Verschlüsselung verwendet wurde, wird in der Kopfzeile der Nachricht im Nur-Text-Format übertragen. Der Empfänger bestimmt anhand dieses Indizes, welcher der 4 Schlüssel zur Entschlüsselung verwendet werden muss.

Es ist nicht erforderlich, dass beide Seiten (in der Regel das RLM und die SIMATIC NET IWL-Station) den gleichen aktiven Satz mit 4 Schlüsseln besitzen. Wenn ein übereinstimmender Schlüssel vorhanden ist, können die Geräte miteinander kommunizieren, sofern beide Geräte diesen gemeinsamen Schlüssel verwenden.



HINWEIS:

Der 802.11-Standard definiert auch die Möglichkeit der Verwendung eines eindeutigen Schlüssels für jede Station, der an die MAC-Adresse der jeweiligen Station gebunden ist. Das SIMATIC NET IWL unterstützt diese Eigenschaft der WEP-Standardfunktion jedoch nicht.

Bei der Planung der Verwendung verschiedener Schlüssel über einen bestimmten Zeitraum müssen die folgenden Aspekte berücksichtigt werden:

- Die Verwendungsdauer eines Schlüssels;
  Dies ist ein direkter Kompromiss zwischen der Sicherheitsstufe (= die Möglichkeit, dass der Schlüsselwert Unberechtigten bekannt wird) und den Betriebskosten
  (= dem Aufwand für die Neukonfiguration der Access Point RLMs und der SIMATIC NET IWL-Stationen).
- Die Anforderungen für einen nahtlosen Übergang von einem Schlüssel zum anderen.
- Die Einschränkung der Zugänglichkeit von Schlüsselwerten für Endbenutzer.

Erweiterte Sicherheitsmaßnahmen

Die vom 802.11-Standard und vom SIMATIC NET IWL bereitgestellten Schlüsselrotationsmöglichkeiten lassen eine Reihe von Szenarien zu, in denen jeweils verschiedene Werte verwendet werden, um den oben genannten Aspekten gerecht zu werden.

Die zeitliche Reihenfolge der Schlüsselkonfigurationseinstellungen auf dem Radio Link-Modul (als AP=Access Point angegeben) und auf der SIMATIC NET IWL-Station (als STA angegeben) ist in verschiedenen Tabellen weiter hinten in diesem Abschnitt angegeben. Die einzelnen Tabellen geben jeweils eine bestimmte Schlüsselrotationsstrategie wieder. Beachten Sie, dass die Spalte "Ausgangs-Schl." zeigt, welcher Schlüssel für die Verschlüsselung von Datenverkehr vom AP zur STA verwendet wird, und dass die Spalte "Eingangs-Schl." zeigt, welche(r) Schlüssel zulässig sind und zum Verschlüsseln von Datenverkehr von der STA zum AP verwendet werden. Die konfigurierten WEP-Schlüssel werden in der Reihefolge der Indexnummer 1-2-3-4 aufgeführt. Die Spalte "Tx" ist die für die Übertragung konfigurierte Indexnummer. Die Schlüsselwerte sind mit Großbuchstaben für echte Schlüssel oder mit einer Null für nicht-konfigurierte Indizes gekennzeichnet.

Die Spalte "Schlüssel 1-2-3-4" enthält ein Gleichheitszeichen (=), wenn sich der Wert nicht vom vorhergehenden Zeitraum unterscheidet. Dies ist inbesondere relevant für die Stationsschlüssel, da beabsichtigt ist, dass die Endbenutzer in der Regel keine Kenntnis von den Schlüsselwerten erlangen und die Station einer IT-Abteilung übergeben müssen, damit die Schlüsselwerte geändert werden. Außerdem soll die Aktion zum Ändern des Tx-Schlüsselindex zu einer Aktion werden, die von den Endbenutzern ausgeführt werden kann, da hierbei keine geheimen Informationen offengelegt werden.

Es wird zwischen drei Schlüsselrotationsstrategien unterschieden:

- 7.5.2.1 Einzelschlüssel - Ohne Übergangszeitraum (Seite 207),
- 7.5.2.2 Einzelschlüssel - Übergangszeitraum (Seite 209) und
- 7.5.2.3 Alternative Schemata (Seite 211).

7.5.2.1 Einzelschlüssel - Ohne Übergangszeitraum

Tabelle 4 Einzelschlüssel - Ohne Übergangszeitraum zeigt ein System, bei dem zu jedem Zeitpunkt nur jeweils ein Schlüssel verwendet wird. Der zu verwendende Schlüssel wird durch die AP-Einstellungen bestimmt, wobei nur ein gültiger Schlüssel für jeden Zeitraum verwendet wird. Dies macht einen Wechsel der Schlüssel auf allen Stationen erforderlich, der mehr oder weniger synchron mit den Änderungen der Radio Link-Modul-Konfiguration erfolgt. Dies ist jedoch umständlich. Daher werden vier Schlüssel verwendet.

Tabelle 4 Einzelschlüssel - Ohne Übergangszeitraum

Zeitraum		AP-Konfiguration		Ausgangs-Schl.	STA-Konfiguration(en)		Eingangs-Schl.
#	Beschreibung	Schlüssel 1-2-3-4	Tx		Schlüssel 1-2-3-4	Tx	
0	Hauptschlüssel A	A-0-0-0	1	A	A-B-C-D	1	A
1	Hauptschlüssel B	0-B-0-0	2	B	=	2	B
2	Hauptschlüssel C	0-0-C-0	3	C	=	3	C
3	Hauptschlüssel D	0-0-0-D	4	D	=	4	D
4	Hauptschlüssel E	E-0-0-0	1	E	E-F-G-H	1	E
5	Hauptschlüssel F	0-F-0-0	2	F	=	2	F

Wenn zunächst alle Stationen mit den Schlüsseln für die ersten 4 Zeiträume konfiguriert werden, muss nur der Tx-Schlüsselindex auf allen Stationen für die ersten drei Schritte geändert werden. Beim Wechsel vom Zeitraum 3 zum Zeitraum 4 müssen die Schlüssel auf allen STAs geändert werden.

7.5.2.2 Einzelschlüssel - Übergangszeitraum

Um einen Übergangszeitraum zwischen den einzelnen Verwendungszeiträumen der Hauptschlüssel einzufügen, muss das Schema, wie in Tabelle 5 Einzelschlüssel - Übergangszeitraum ersichtlich, geändert werden.

Tabelle 5 Einzelschlüssel - Übergangszeitraum

Zeitraum		AP-Konfiguration		Aus-gangs Schl.	STA-Konfiguration(en)		Ein-gangs Schl.
#	Beschreibung	Schlüssel 1-2-3-4	Tx		Schlüssel 1-2-3-4	Tx	
0	Hauptschlüssel A	A-0-0-0	1	A	A-B-C-D	1	A
1	Übergang A-B	A-B-0-0	2	B	=	1|2	A | B
2	Hauptschlüssel B	0-B-0-0	2	B	=	2	B
3	Übergang B-C	0-B-C-0	3	C	=	2|3	B | C
4	Hauptschlüssel C	0-0-C-0	3	C	=	3	C
5	Übergang C-D	0-0-C-D	4	D	=	3|4	C | D
6	Hauptschlüssel D	0-0-0-D	4	D	=	4	D
7	Übergang D-E	E-0-0-D	1	E	A-B-C-DE-F-G-H	4|1	D | E
8	Hauptschlüssel E	E-0-0-0	1	E	E-F-G-H	1	E
9	Übergang E-F	E-F-0-0	2	F	=	1|2	E | F

Beachten Sie, dass die Endbenutzer in den Übergangszeiträumen 1, 3 und 5 von einem Tx-Schlüsselindex zum nächsten wechseln können. Am Ende dieses Zeitraums müssen alle Stationen zum neuen Schlüsselindex gewechselt haben. Der Übergangszeitraum 7 beinhaltet außerdem den

Übergang zu einem neuen Schlüsselsatz. Die Gesamtgültigkeitsdauer eines verwendeten Schlüssels setzt sich aus der Hauptgültigkeitszeit und zwei Übergangszeiträumen zusammen. Da angenommen wird, dass die Hauptgültigkeitszeit viel länger ist als die Übergangszeit, kann dieses Schema trotzdem als Einzelschlüsselschema betrachtet werden, weil die meiste Zeit nur jeweils ein Schlüssel in Verwendung ist.

7.5.2.3 Alternative Schemata

Es können alternative Schemata mit Hauptgültigkeitszeiträumen verwendet werden, während denen zwei oder mehr Schlüssel aktiv sind. Ein Beispiel hierfür finden Sie in Tabelle 6 Alternative Schemata.

Tabelle 6 Alternative Schemata

Zeitraum		AP-Konfiguration		Aus-gangs Schl.	STA-Konfiguration(en)		Ein-gangs Schl.
#	Beschreibung	Schlüssel 1-2-3-4	Tx		Schlüssel 1-2-3-4	Tx	
0	Hauptschlüssel A	A-0-0-0	1	A	A-B-C-D	1	A
1	Hauptschlüssel A+B	A-B-0-0	2	B	=	1|2	A | B
2	Hauptschlüssel B+C	0-B-C-0	3	C	=	2|3	B | C
3	Hauptschlüssel C+D	0-0-C-D	4	D	=	3|4	C | D
4	Hauptschlüssel D+E	E-0-0-D	1	E	A-B-C-D E-F-G-H	4 1	D E
5	Hauptschlüssel E+F	E-F-0-0	2	F	E-F-G-H	1|2	E | F

Tabelle 6 Alternative Schemata zeigt ein Schema, bei dem in jedem Zeitraum jeweils zwei Schlüssel in Verwendung sind. Am Ende des Zeitraums wird der älteste Schlüssel ungültig und muss auf allen Stationen ersetzt werden. Der Vorteil dieses Schemas gegenüber dem Schema in Tabelle 5 besteht darin, dass weniger häufig Konfigurationsänderungen an allen Radio Link-Modulen vorgenommen werden müssen.

8 Erweiterte Netzwerkkonfiguration

8.1 Einführung

Wenn Sie SIMATIC NET IWL-Netzwerk über die Standardkonfiguration hinaus konfigurieren wollen, sollten Sie mit einigen weiterführenden Aspekten vertraut sein:

- Erweiterte Parameter (Seite 213),
- Konfiguration großer Netzwerke (Seite 242),
- Ändern der Konfiguration (Seite 253),
- Wiederherstellen einer gesicherten Konfiguration (Seite 255),
- Duale PC Card Konfiguration (Seite 256),
- Über IP-Adressen und Subnetze (Seite 257).

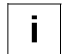
8.2 Erweiterte Parameter

Unter Umständen kann es sinnvoll sein, die von Ihren Radio Link-Modulen unterstützten Optionen der “Erweiterten Parameter” näher zu betrachten. Dies gilt insbesondere dann, wenn Sie größere Netzwerke betreuen, die über mehr als zehn Radio Link-Module enthalten.

Zu den erweiterten Parametern zählen:

- Erweiterte Parameter wie beispielsweise RTS/CTS Medium Reservation oder der Abstand zwischen Access Point RLMs
- Bridge-Parameter, mit deren Hilfe Sie spezifische Netzwerkprotokolle oder den Datenverkehr zwischen spezifischen Stationen filtern können.
- Access Point RLM-Parameter, oder
- SNMP-Parameter.

In den meisten Netzwerken sorgen die Standardeinstellungen der erweiterten Parameter für eine überaus zuverlässige Netzwerkkonnektivität. Sie sollten diese Paramter nur ändern, wenn Sie mit der Technologie und der Wirkungsweise der Parameter vertraut sind, zum Beispiel aufgrund Ihrer Erfahrung und der Kenntnis ähnlicher Parameter in herkömmlichen Netzwerkumgebungen und/oder in SIMATIC NET IWL-Netzwerkumgebungen.



HINWEIS:

Einige der im Folgenden beschriebenen erweiterten Parameter sind möglicherweise als “allgemeine” Parameter gekennzeichnet. Dies bedeutet, dass Sie in allen Ihren Radio Link-Modulen Ihres

Netzwerks identisch sein sollten (siehe auch Konfiguration großer Netzwerke (Seite 242)).

Um die erweiterten Parameter einzurichten und eine Verbindung zu dem zu konfigurierenden Access Point Radio Link-Modul herzustellen, folgen Sie einfach den im vorigen Kapitel Konfigurieren von Infrastruktur-Netzwerken (Seite 62) beschriebenen Anweisungen.

8.2.1 Erweiterte Parameter

Wenn Sie für ein Access Point Radio Link-Modul eine Standardkonfiguration erstellt haben, wie es im vorherigen Abschnitt beschrieben ist, sind Ihnen unter Umständen schon die zusätzlichen Schaltfächen im Setup-Fenster aufgefallen. Sie sind auch in der Registerkarte Wireless Interfaces im Fenster RLM Manager (Seite 69) dargestellt.

8.2.1.1 Frequenz

Das Menü Frequency Setup erlaubt es Ihnen, eine Betriebsfrequenz aus einer Reihe von Unterkanälen innerhalb des 2.4 GHz-Frequenzbands auszuwählen.
Die Anzahl der verfügbaren Kanäle wird von den in Ihrem Land gültigen Fernmeldebestimmungen begrenzt.

Klicken Sie im Editiermodus auf der Registerkarte **Wireless Interfaces** auf die Schaltfläche **Advanced**, um die Frequenzparameter zu ändern.

Zur Optimierung des Netzwerkverkehrs wird empfohlen, Radio Link-Modulen, die benachbarte drahtlose Zellen versorgen, unterschiedliche Betriebsfrequenzen zuzuweisen. Damit werden die Stationen in jeder der

Zellen die maximale Bandbreite, die in dieser Zelle zur Verfügung steht, nutzen können.

Drahtlose Stationen, die mit Wireless Client Adapters (CP 1515) ausgestattet sind, können den Betriebskanal dynamisch ändern, wenn sie sich zwischen Access Points (RLMs) bewegen, die mit unterschiedlichen Unterkanälen arbeiten. Dieses Merkmal ist nur für WaveLAN IEEE 802.11 Karten. Legacy WaveLAN Produkte können sich nur inerhalb von Einzelkanalkonfigurationen bewegen.

8.2.1.2 RTS/CTS-Medienreservierung

Die RTS/CTS-Medienreservierung bietet möglicherweise eine Lösung für Netzwerke, in denen:

- die Dichte der Stationen und Access Points (RLMs) sehr niedrig ist,
- Sie aufgrund starker Framekollisionen bei den Radio Link-Modulen eine niedrige Netzwerk-Performance feststellen.

Jedoch dürfte es in den meisten Netzwerkumgebungen höchst unwahrscheinlich sein, dass auf den Access Point Radio Link-Modulen eine Aktivierung der RTS/CTS-Medienreservierung notwendig ist, um Kollisionen auf diese Weise zu verhindern. Es wird empfohlen, vor einer Änderung dieser Access Point RLM-Einstellung die Informationen über Optimierung von drahtgebundenen Verbindungen (Seite 133) zu lesen.

Klicken Sie auf der Registerkarte **Wireless Interfaces** die Schaltfläche **Advanced**, um die RTS/CTS-Medienreservierung zu aktivieren.

8.2.1.3 Störungsunempfindlichkeit

Die Störungsunempfindlichkeit kann in Ausnahmefällen aktiviert werden, wenn Sie eine niedrige Netzwerkleistung verbessern wollen und dieses Problem möglicherweise mit Störungen innerhalb des Bandes (zum Beispiel von Mikrowellengeräten) zusammenhängt. Störungen machen sich üblicherweise durch ein schlechtes Singal-/Rauschverhältnis bemerkbar, das auf einem guten Signalpegel und einem hohen Rauschpegel basiert. Dieses Verhalten tritt häufig auf, wenn:

— die “gestörte” Stationen oder das “gestörte” Radio Link-Modul sich in unmittelbarer Nähe zu einer Störquelle befindet, oder

— sich die Störquelle im Signalweg zwischen der “gestörten” Station und dem Access Point Radio Link-Modul befindet.

Um die Störungsunempfindlichkeit zu aktivieren, klicken Sie im Editiermodus auf der Registerkarte **Wireless Interfaces** auf die Schaltfläche **Advanced**, und aktivieren Sie danach die Option **Interference Robustness**.

8.2.1.4 Abstand zwischen Access Points (APs)

Falls der Datenbedarf der Benutzer in Ihrer Netzwerkumgebung sehr hoch ist, oder falls sich in Ihrer Netzwerkumgebung auf kleiner Fläche sehr viele Benutzer befinden, ist es unter Umständen ratsam, die Anzahl der Access Points (RLMs) zu erhöhen und damit den Abstand zwischen den Radio Link-Modulen zu verringern. Danach können Sie den Parameter "Distance between Access Points" anpassen, um die Kommunikationslast der drahtlosen Stationen auf die Access Point Radio Link-Module optimaler zu verteilen.

Klicken Sie im Editiermodus auf der Registerkarte **Wireless Interfaces** auf die Schaltfläche **Advanced**, um den Parameter "Distance between APs" zu ändern. Im Feld **Distance between Access Points** können Sie aus folgenden drei Optionen auswählen:

- Large (Standard)
- Medium
- Small

Die Standardeinstellung **Large** bietet maximale drahtlose Netzabdeckung bei einer geringen Anzahl von Access Points (RLMs). Diese Option wird üblicherweise in Netzwerken mit nur einer Zelle verwendet, stellt aber auch eine effiziente und kostengünstige Lösung für die meisten Netzwerke dar, die über mehrere drahtlose Zellen verfügen.



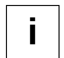
ACHTUNG:
Die Einstellung für den Abstand zwischen Radio Link-Modulen muss auf allen mit SIMATIC NET IWL ausgerüsteten Geräten in Ihrem Netzwerk gleich sein. Unterschiedliche Konfigurationseinstellungen dieses Parameters können zu unvorhersehbaren Ergebnissen und Leistungsdefiziten bei den drahtlosen (mobilen) Stationen in Ihrem Netzwerk führen.

Treten in einer Umgebung, in der eigentlich eine ausgezeichnete Netzqualität gemessen wurde, dennoch Verzögerungen in der Netzwerkreaktionszeit auf, so können Sie **Medium** als Abstand zwischen

Access Points (RLMs) auswählen. Langsame Netzwerkreaktionszeiten können in Umgebungen auftreten, in denen:

- sich eine große Anzahl drahtloser Stationen auf engem Raum befindet und dadurch Verzögerungen in den Datenübertragungen auftreten,
- eine Anzahl drahtloser Stationen aufgrund ihres hohen Datenaufkommens den Datenverkehr anderer Stationen verzögern,
- die Einstellung **Large** zu Überlappungen der Funkzellen führt, sodass Stationen in einer Zelle die Datenübertragung von Stationen in einer anderen Zelle verzögern.

Einen **geringen** Abstand (small) zwischen Radio Link-Modulen sollten Sie nur wählen, wenn Sie eine Drahtlos-Infrastruktur entwerfen, die über eine große Anzahl von Access Points (RLMs) verfügen wird: wenn zum Beispiel die gesamten Investitionskosten für Hardware weniger kritisch sind als der maximale Datendurchsatz pro Zelle.



HINWEIS:

Die Einstellungen **Medium** oder **Small** für den Abstand zwischen Access Points (RLMs) setzen eine erstklassige Signalqualität innerhalb der gesamten abzudeckenden Fläche voraus. Wurde in einer Umgebung die tatsächliche Verteilung der Radio Link-Module so gewählt, dass bei einer möglicht geringen Anzahl von Access Points (RLMs) eine maximale Flächenabdeckung erreicht wird, führt eine Änderung des Abstands zwischen RLMs von **Large** zu **Medium** oder **Small** nicht zu besseren Ergebnissen. Ganz im Gegenteil könnte damit die Roaming-Leistungsfähigkeit Ihrer drahtlosen Stationen ernsthaft beeinträchtigt werden, und “Out-of-

Range"-Situationen könnten zu Kommunikationsfehlern im Netzwerk führen.

Sollten Sie erwägen, als Abstand zwischen Radio Link-Modulen die Option **Medium** oder **Small** zu wählen, um ein hochperformantes Netzwerk zu erstellen, sollten Sie zudem den Abschnitt Verwaltung der Frequenzkanäle (Seite 153) lesen.

Weitere Informationen zur Dichte von Access Point RLMs finden Sie in Abschnitt Optimierung der Leistungsfähigkeit (Seite 126).

8.2.1.5 Multicast-Geschwindigkeit

Die Multicast-Geschwindigkeit bezeichnet die bevorzugte Übertragungsgeschwindigkeit Ihres Access Point Radio Link-Moduls, wie er vom Radio Link weitergeleitet wird. Auch wenn niedrigere Übertragungsraten in der Regel verlässlicher sind, ist es unter Umständen sinnvoll, höheren Datendurchsatz gegenüber größerer Reichweite Ihres drahtlosen Funksignals vorzuziehen.

Weitere Informationen zur Multicast-Geschwindigkeit finden Sie in der Online-Hilfe des RLM Manager-Programms.

8.2.2 Bridge-Parameter

Eine Methode zur Optimierung der Leistung Ihres drahtlosen Netzwerks ist es, "unnötigen" Verkehr zu vermeiden und nicht über das drahtlose Netzwerk zu übertragen. Unnötiger Verkehr umfasst:

- Spezifische Netzwerkprotokolle, die zwischen Netzwerkgeräten wie beispielsweise Servern ausgetauscht werden und für die drahtlosen Stationen nicht von Bedeutung sind,
- Broadcast- und/oder Multicast-Meldungen, die von spezifischen Netzwerkgeräten wie beispielsweise Servern ausgetauscht werden und nicht ausdrücklich an die drahtlosen Stationen adressiert sind,
- "Junk Traffic," wie beispielsweise Fehlermeldungen, die von fehlerhaften Geräten erzeugt werden, oder Verkehr, der das Ergebnis von (vermeidbaren) fehlerhaften Netzwerkkonfigurationen ist (wie beispielsweise geschlossene Netzwerkschleifen).

Das Filtern von unnötigem Verkehr gewährleistet eine ausreichende Bandbreite des drahtlosen Mediums für die drahtlosen Stationen und optimiert damit die Durchsatzeffizienz für diese Stationen.

Mithilfe der Registerkarte **Bridge** können Sie die Leistung des drahtlosen Netzwerks auf folgende Weise optimieren:

- Filterung von Protokollen, um zu verhindern, dass spezifische Netzwerkprotokolle in das Wireless-LAN übertragen werden (siehe Protokolfilterung (Seite 223)).
- Filterung des Verkehrs zwischen zwei spezifischen Stationen, die durch ihre statische MAC-Adresse eindeutig identifiziert werden können (siehe Statischer MAC-Adressfilter (Seite 225)).
- Aktivierung des Spanning Tree-Mechanismus, um Fehler durch geschlossene Netzwerkschleifen zu lösen (siehe Spanning Tree (Seite 226)).

- Begrenzung der Anzahl zu bridgender Meldungen pro Port und/oder Stationen (Storm Threshold Filtering, siehe Storm-Schwellenwert (Seite 228)).



ACHTUNG:
Die Einstellungen der Bridge-Parameter sind typische“allgemeine” Parameter, d.h. die Einstellungen der Bridge-Parameter sollten auf allen Access Points (RLMs) identisch sein.

Abbildung 36 Die Registerkarte "Bridge" im Editiermodus



Um die Bridge-Parameter einzurichten, verbinden Sie sich mit dem Access Point RLM und wählen Sie die Registerkarte **Bridge**, um die Bridge-Parameter wie in Abbildung 36 Die Registerkarte "Bridge" im Editiermodus dargestellt anzuzeigen.

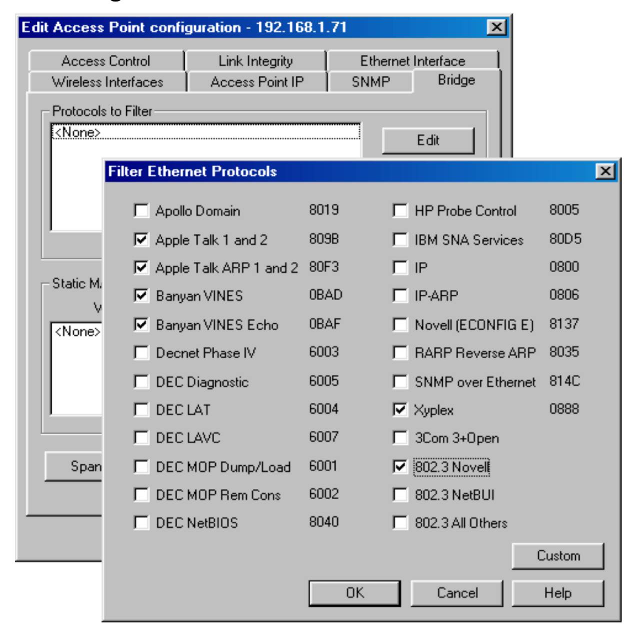
8.2.2.1 Protokolfilterung

In der oberen Hälfte der Registerkarte **Bridge** werden die gefilterten Protokolle aufgeführt. Standardmäßig werden im Radio Link-Modul keine Protokolle (**<None>**) gefiltert, sodass alle Protokolle innerhalb des drahtlosen Medium übertragen werden können. Dies ist die empfohlene Einstellung, sofern Sie nicht bestimmten Protokolle ausfiltern müssen.

Gehen Sie folgendermaßen vor, um Protokolle zu filtern:

1. Ermitteln Sie, welche Protokolle unbedingt gebridgt werden müssen.
2. Klicken Sie auf die Schaltfläche **Edit**, um das Fenster "Filter Ethernet Protocols" wie in Abbildung 37 Zu filternde Ethernet-Protokolle auswählen dargestellt anzuzeigen.

Abbildung 37 Zu filternde Ethernet-Protokolle auswählen



3. Aktivieren Sie das Kontrollkästchen der Protokolle, die nicht über das drahtlose Medium übertragen werden müssen.

Deaktivieren Sie das Kontrollkästchen, um das Filtern dieses spezifischen Protokolls wieder aufzuheben.

4. Optional: Wenn Sie ein Protokoll filtern wollen, das nicht in der Liste aufgeführt ist, klicken Sie auf die Schaltfläche **Custom**, und geben Sie das Protokoll von Hand ein.
5. Klicken Sie auf **OK**, wenn Sie alle Eingaben abgesclossen haben. Damit kehren Sie zur Registerkarte **Bridge** zurück (siehe Abbildung 36 Die Registerkarte "Bridge" im Editiermodus).

   Alle von Ihnen gewählten Protokolle und alle von Ihnen manuell eingetragenen benutzerspezifischen Protokolle werden nun in der Liste **Protocols to Filter** aufgeführt.
6. Sie können nun eine der anderen Bridge-Parameteroptionen wählen, andere Parameter anpassen oder auf **OK** klicken, um Ihre Einstellungen zu speichern und zum Hauptfenster des RLM Manager zurückzukehren.

8.2.2.2 Statischer MAC-Adressfilter

Um den Datenverkehr zwischen Stationen auszufiltern, der nicht über die drahtlose Schnittstelle gesendet oder empfangen werden muss, können Sie in der unteren Hälfte der Registerkarte **Bridge** im Feld **Static MAC address Filter** statische Filter für MAC-Adressen festlegen. Der Standardwert **<None>** ist für die meisten Netzwerkumgebungen geeignet (siehe Abbildung 36 Die Registerkarte "Bridge" im Editiermodus).

Sie können die Option der MAC-Filterung beispielsweise dazu verwenden, Broadcast- oder Mulitcast-Meldungen, die zwischen mit Kabel verbundenen Servern ausgetauscht werden (die also über das herkömmliche Netzwerkkabel kommunizieren können), auszufiltern.

Tragen Sie die MAC-Adressen beider Geräte als Paar in die Liste **Static MAC address Filter** ein, um den Datenaustausch zwischen diesen Geräten auszufiltern.

Sendet eine der aufgeführten Stationen ein Telegramm an eine MAC-Adresse, die in der Liste der MAC-Adresspaare aufgeführt ist, leitet der Access Point RLM das Telegramm nicht über die drahtlose Station weiter. Alle Übertragungen, die eine Station an eine andere nicht aufgeführte MAC-Adresse senden möchte, werden weitergeleitet.

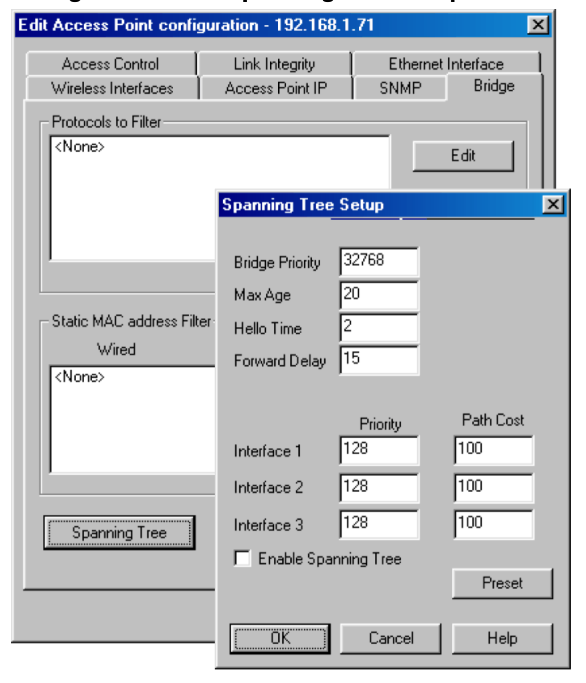
Weitere Informationen über das statische Filtern von MAC-Adressen finden Sie im Abschnitt Optimierung der Leistungsfähigkeit (Seite 126).

8.2.2.3 Spanning Tree

Die Schaltlfäche **Spanning Tree** erlaubt es Ihnen, Parameter festzulegen, auf welche Weise der optimale Weg für Datenströme im Netzwerk ermittelt werden soll.

Sie können Spanning Tree in Netzwerken verwenden, die im Konzept bereits Schleifen vorsahen, wie zum Beispiel eine redundante kabelbasierte Verbindung als Backup für eine drahtlose Hauptverbindung.

Abbildung 38 Fenster "Spanning Tree Setup"



Gehen Sie folgendermaßen vor, um Spanning Tree zu aktiveren:

Erweiterte Parameter

1. Klicken Sie auf die Schaltfläche **Spanning Tree**, um das Fenster "Spanning Tree Setup" zu öffnen (siehe Abbildung 38 Fenster "Spanning Tree Setup").
2. Aktivieren Sie das Kontrollkästchen **Enable Spanning Tree**.
3. Verwenden Sie die Standardeinstellungen (siehe Abbildung 38 Fenster "Spanning Tree Setup").
4. Klicken Sie auf **OK**, um diese Einstellung zu bestätigen und zur Registerkarte **Bridge** zurückzukehren.
5. Klicken Sie nochmals auf **OK**, um diese Einstellungen zu speichern und zum Hauptfenster des RLM Manager zurückzugelangen. Andernfalls fahren Sie fort und ändern Sie weitere Parameter.

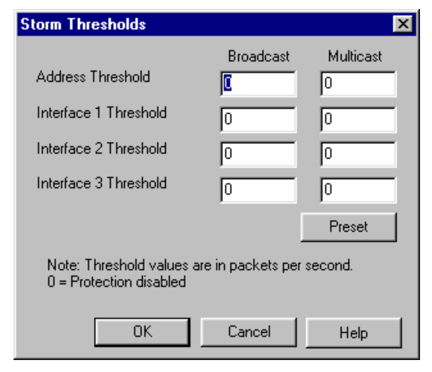
An dieser Stelle ist es ratsam, eine Sicherheitskopie zu erstellen (siehe Schritt 4 - Erstellen einer Sicherungsdatei der Konfiguration (Seite 72)).

8.2.2.4 Storm-Schwellenwert

Die Schaltfläche **Storm Thresholds** erlaubt es Ihnen, Parameter festzulegen, um das Netzwerk vor einer Überlastung durch Telegramme von einzelnen Stationen oder via einen spezifischen Port zu schützen.

Mithilfe des Fensters **Storm Thresholds** können Sie festlegen, wie viele Multi- und Broadcast-Meldungen von einem Port (oder einer Adresse) pro Sekunde maximal übertragen und weitergeleitet werden .

Abbildung 39 Deaktivierter Storm Threshold-Schutz



Standardmäßig ist der Storm-Schutz deaktiviert (alle Schwellenwert betragen 0).

1. Falls Sie einen Schwellenwert für einen Storm-Schutz benötigen und sich nicht sicher sind, welche die korrekten Boradcast- und Multicastwerte sind, klicken Sie auf die Schaltfläche **Preset**. Dies richtet Schwellenwerte ein, die für die meisten Netzwerkumgebungen angemessen sind.
2. Klicken Sie auf **OK**, um diese Einstellungen beizubehalten und zur Registerkarte **Bridge** zurückzukehren.

Klicken Sie nochmals auf **OK**, um diese Einstellungen zu speichern und zum Hauptfenster des RLM Manager zurückzugelangen. Andernfalls fahren Sie fort und ändern Sie weitere Parameter.

8.2.3 Access Point IP-Parameter

Die Registerkarte für die Access Point RLM IP-Parameter erlaubt es Ihnen, die allgemeinen IP-Parameter festzulegen und die eindeutige IP-Adresse Ihres Radio Link-Moduls zu ändern.

Gehen Sie folgendermaßen vor, um die IP-Parameter zu ändern:

1. Stellen Sie sicher, dass Sie mit dem richtigen Access Point Radio Link-Modul verbunden sind, und wählen Sie im Editiermodus die Registerkarte **Access Point IP**, um die IP-Parameter anzuzeigen (siehe Abbildung 40 IP-Parameter des Radio Link-Moduls einrichten).
2. Prüfen und/oder ändern Sie die Parameter Ihrer Wahl.

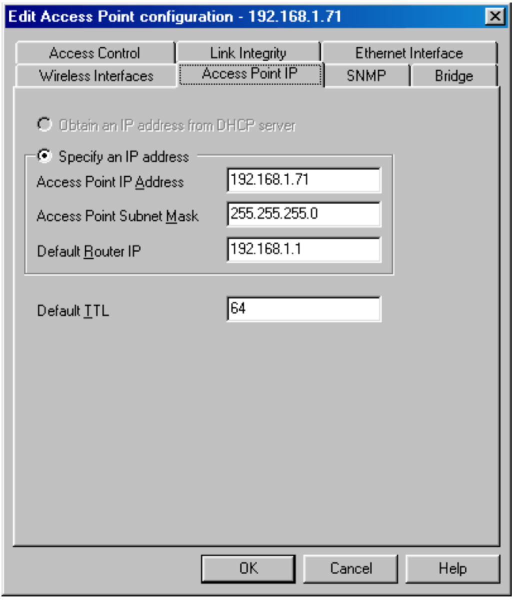
   Folgende Parameter müssen angegeben werden:

   - **"IP-Adresse"** des Radio Link-Moduls (jedes Access Point RLM besitzt eine eindeutige IP-Adresse; falls ein BOOTP- oder DHCP-Server vorhanden ist, wird diese IP-Adresse automatisch eingetragen).
   - **"Subnetzmaske"** des Access Point RLM (sie ist für alle Radio Link-Module identisch; falls ein BOOTP- oder DHCP-Server vorhanden ist, wird diese IP-Adresse automatisch eingetragen).
   - Optional: **Standard-Router** (ist üblicherweise bei allen Access Points (RLMs) gleich).
   - Optional: **Default TTL** (Time To Live) ; ist üblicherweise bei allen Access Points (RLMs) gleich.

   Alle Parameter werden in den folgenden Absätzen erläutert.

3. Wenn Sie alle Einstellungen vorgenommen haben, können Sie andere Parameter anpassen oder auf **OK** klicken, um Ihre Einstellungen zu speichern und zum Hauptfenster des RLM Manager zurückzukehren.

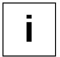
Abbildung 40 IP-Parameter des Radio Link-Moduls einrichten



8.2.3.1 IP-Adresse

Jeder Access Point RLM benötigt eine eindeutige IP-Adresse. Verwenden Sie entweder:

- DHCP, um eine IP-Adresse automatisch zu beziehen, oder
- geben Sie eine IP-Adresse von Hand ein.



HINWEIS:

Um jedes Radio Link-Modul spezifisch ansprechen zu können, muss jeder Access Point (RLMs) über eine eindeutige IP-Adresse verfügen. Doppelt vergebene IP-Adressen können zu unerwartetem Netzwerkverhalten führen und/oder die Leistungsfähigkeit des Netzwerks stark beeinträchtigen.

8.2.3.1.1 Eine IP-Adresse manuell zuweisen

Falls Sie eine IP-Adresse manuell zuweisen wollen, verwenden Sie das Feld "Access Point RLM **IP Address**", um einen Wert einzugeben, der innerhalb des in Ihrer Organisation gültigen IP-Raums liegt.

Die IP-Adresse wird vorrangig zur Kommunikation mit dem Access Point RLM verwendet, wenn Sie das Gerät mithilfe des RLM Manager-Programm überwachen oder konfigurieren.

Falls Ihre Organisation keine IP-Adressen verwendet, können Sie einen benutzerdefinierten Wert eintragen, beispielsweise einen Wert nach dem selben Muster der standardmäßig voreingestellten IP-Adresse 153.69.254.254, wobei Sie die letzten drei Ziffern mit ein Wert zwischen “1” und “253” ersetzen.

8.2.3.1.2 Eine IP-Adresse automatisch zuweisen

Falls ein DHCP-Server in Ihrem Netzwerk verfügbar ist, wird dem Radio Link-Modul automatisch vom DHCP-Server eine IP-Adresse zugewiesen. Aktivieren Sie auf der Registerkarte **Access Point IP** die Option **Obtain an IP-Adresse from DHCP server**, um das automatische Beziehen einer IP-Adresse vom DHCP-Server zu ermöglichen.

Weitere Informationen zu DHCP finden Sie in Abschnitt BOOTP und DHCP (Seite 258).

8.2.3.2 Subnetzmaske

Das Feld **RLM Subnetzmaske** ist ein allgemeiner Parameter und muss bei ALLEN Netzwerkgeräten innerhalb Ihres IP-Subnetzes identisch sein.

Verwenden Sie entweder den Standardwert (255.255.0.0), oder ändern Sie die Subnetzmaske auf den Wert, der Ihrem Netzwerk entspricht.

Falls die Option **Obtain an IP-Adresse from DHCP server** aktiviert ist, wird auch die Subnetzmaske automatisch eingetragen.

8.2.3.3 Standard-Router

Das Feld **Default Router IP** ist ein optionales Feld und ist nur relevant, wenn Sie die Unterstützung der Radio Link-Module für TRAP-Nachrichten verwenden wollen (siehe auch SNMP-Parameter (Seite 234)).

Mithilfe des Felds "Default Router IP" können Sie die IP-Adresse des Routers festlegen, den das Radio Link-Modul zur Suche nach Trap Host-IP-Adressen verwendet (im SNMP-Parameter angegeben).

Der Standard-Router und die Trap Host IP-Adresse, die später in diesem Kapitel beschrieben werden, werden nur für TRAP-Nachrichten verwendet, die von dem Access Point Radio Link-Modul bei einem Reset, einer Änderung der Konfiguration oder einem erzwungenen Neustart erzeugt werden.

Ist der Wert im Feld **Default Router IP** auf 0.0.0.0 gesetzt (Standardwert), so werden von diesem Radio Link-Modul keine Trap-Nachrichten initiiert.

Der Standard-Router ist auch wichtig, wenn Sie das Radio Link-Modul aus einem anderen Subnetz heraus verwalten oder einfach nur anpingen wollen.

8.2.3.4 Time To Live (TTL)

Das Feld **Default TTL** (Time To Live) legt die maximale Anzahl Hops für eine IP-Nachricht, die vom Access Point RLM erzeugt wurde, fest (wird üblicherweise für Trap Host-Nachrichten verwendet).

Dieser Wert wird jedes Mal um eins verringert, wenn die Nachricht einen Router passiert. Wenn der TTL-Wert 0 wird, wird die Nachricht vom nächsten Router, auf den sie trifft, verweigert. Standardmäßig beträgt dieser Wert 64.

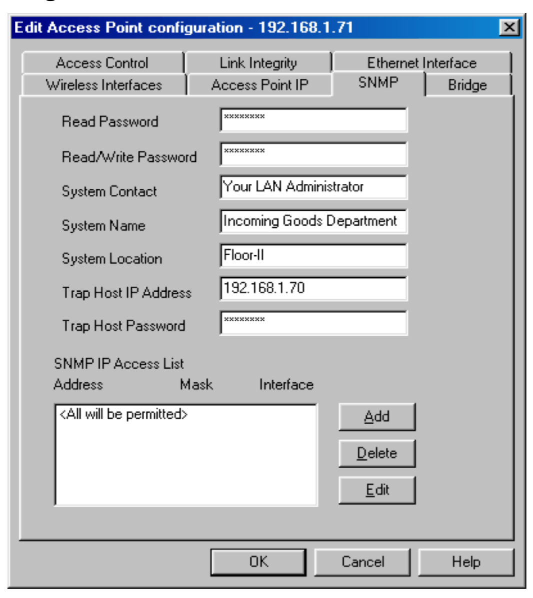
8.2.4 SNMP-Parameter

Die meisten SNMP-Parameter (mit Ausnahmen von "System Location" und "System Name") sind allgemeine Parameter, d.h. sie müssen bei ALLEN Radio Link-Modulen in Ihrem Netzwerk identisch sein.

Gehen Sie folgendermaßen vor, um die SNMP-Parameter festzulegen:

1. Stellen Sie sicher, dass Sie mit dem korrekten Access Point Radio Link-Modul verbunden und wählen Sie die Registerkarte **SNMP**, um die SNMP-Parameter wie in Abbildung 41 SNMP-Parameter einrichten dargestellt anzuzeigen.

Abbildung 41 SNMP-Parameter einrichten



2. Prüfen und/oder ändern Sie die Parameter Ihrer Wahl.

   Dabei sollten Sie folgende Parameter angeben:

   - **Read/Write Password**, um den Zugriff auf die Konfiguration Ihrer Access Points (RLMs) zu beschränken, und
   - **System Name**, um eine einfache Identifizierung des Radio Link-Moduls zu ermöglichen, wenn Sie die Diagnoseoptionen Ihres Softwaretools verwenden.

   Diese und alle anderen SNMP-Parameter sind in den folgenden Absätzen beschrieben.

3. Wenn Sie alle Einstellungen vorgenommen haben, können Sie andere Parameter anpassen oder auf **OK** klicken, um Ihre Einstellungen zu speichern und zum Hauptfenster des RLM Manager zurückzukehren.

8.2.4.1 Passwort für Lesevorgänge

Ändern Sie das **Read Password**, um unberechtigte Zugriffe auf die Access Points (RLMs) zu verhindern.

Es ist ein Passwort für Lesevorgänge erforderlich, wenn sie sich mit RLMs unter Verwendung der **Monitor**-Option verbinden. Der Standardwert ist “public.”

Mithilfe des Passworts für Lesevorgänge kann ein lokaler Netzwerkadministrator nur die Statistiken und Tabellen der Radio Link-Module überwachen, jedoch kann er keine dieser Parameter anzeigen oder ändern.

8.2.4.2 Passwort für Lese-/Schreibvorgänge

Ändern Sie den Parameter **Read/Write Password**, um unerlaubten Zugriff auf die RLMs und unberechtigte Änderungen an ihren Konfigurationseinstellungen vorzunehmen, zu verhindern.

Ein Passwort für Lese-/Schreibvorgänge ist erforderlich, um die Schaltfläche **Edit** zu verwenden und sich mit einem Access Point Radio Link-Modul zu verbinden. Der Standardwert ist "public."

Mithilfe des Passworts für Lese-/Schreibvorgänge kann ein lokaler Netzwerkadministrator die Statistiken und Tabellen der Radio Link-Module überwachen und alle Parameter der Konfigurationseinstellungen anzeigen und ändern. Mithilfe unterschiedlicher Werte für das Passwort für Lese- und Lese-/Schreibvorgänge können Sie verschiedene Berechtigungsstufen für Ihre Netzwerkadministratoren festlegen und definieren, inwieweit sie die RLMs überwachen und konfigurieren dürfen.

8.2.4.3 System Contact

Verwenden Sie das Feld **System Contact**, um einen allgemeinen Namen für den Netzwerkadministrator oder die Abteilung einzutragen (z.B. wie in Abbildung 41 SNMP-Parameter einrichten dargestellt "Your LAN Administrator").

8.2.4.4 System Name

Verwenden Sie das Feld **System Name**, um einen allgemeinen logischen Standort für das Access Point Radio Link-Modul anzugeben (z. B. "Incoming Goods Department," wie in Abbildung 41 SNMP-Parameter einrichten dargestellt).

8.2.4.5 System Location

Verwenden Sie das Feld **System Location**, um einen allgemeinen physikalischen Standort des Radio Link-Moduls anzugeben (z.B. "Access Point RLM Etage 1N", wie in Abbildung 41 SNMP-Parameter einrichten dargestellt).

8.2.4.6 Trap Host-IP-Adresse

Wenn Sie vorhaben, das Trap Alert-System wie in Trap Host-Nachrichten (Seite 200) beschrieben einzusetzen, können Sie in das Feld **Trap Host IP Address** die Adresse der Netzwerkmanagement-Station eintragen, die die SNMP Trap-Nachrichten sammeln sollte. Wenn Sie nicht vorhaben, Trap Host Alerts zu verwenden, setzen Sie den Wert auf “0.0.0.0”.

Weitere Informationen über Trap Host-Nachrichten finden Sie im Abschnitt Trap Host-Nachrichten (Seite 200).

8.2.4.7 Trap Host Password

Verwenden Sie das Feld **Trap Host Password**, um ein Kennwort einzugeben, das in SNMP Trap-Nachrichten einbezogen werden wird. Sie können dieses Kennwort verwenden, um bei der Trap Host-Station Trap-Nachrichten auszufiltern, die unter Umständen irrtümlicherweise an die Trap Host-Station gesendet wurden.

8.2.4.8 SNMP IP Access List

Mithilfe der **SNMP IP Access List** können Sie eine zusätzliche Sicherheitsstufe einrichten, die über die Kennwörter für Lese-und Schreib-/ Lesevorgänge hinausgeht. Dies gestattet es einer begrenzten Anzahl LAN-

Administratorstation, auf Basis der IP-Adresse dieser Stationen die Konfiguration der Radio Link-Module anzuzeigen und/oder zu ändern.

Das Feld **SNMP IP Access List** sollte üblicherweise die IP-Adressen aller LAN-Administratorstation enthalten, die den RLM Manager zur Konfiguration und /oder Überwachung von Radio Link-Modulen verwenden.

Um eine LAN-Administratorstation zu autorisieren, müssen Sie folgendes eingeben:

- die IP-Adresse der Station, und
- die Access Point RLM-Netzwerkschnittstelle, über die sie auf das Access Point RLM zugreifen werden.

Um die Schnittstelle anzugeben, verwenden Sie entweder:

- “1” für Ethernet
- “2” für die drahtlose Netzwerkschnittstelle in Socket A, oder
- “3” für die drahtlose Netzwerkschnittstelle in Socket B.

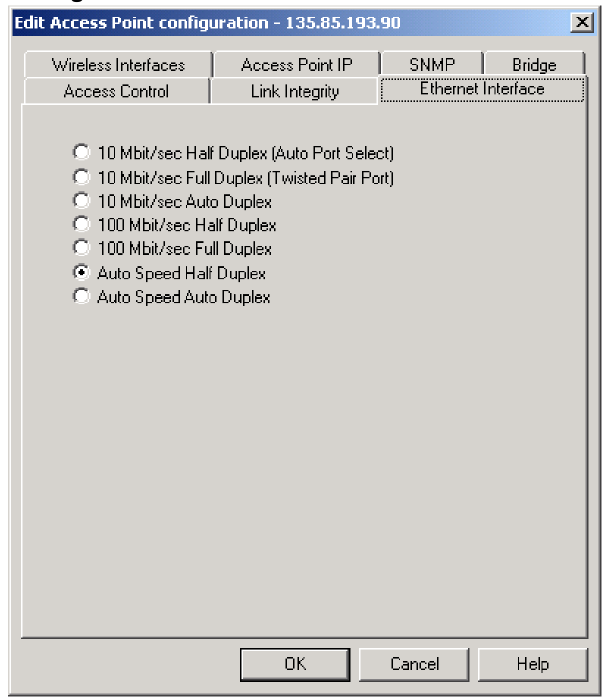
Alternativ können Sie auch den Wert “x” verwenden, um den erkannten IP-Adressen den Zugriff auf die Radio Link-Module zu gestatten.

Um mehreren LAN-Administratorstationen den Zugriff auf die RLM-Konfiguration und die Überwachung der Parameter zu ermöglichen, können Sie auch einen IP-Adressbereich zuweisen. Geben Sie hierzu einen Subnetzmasken-Wert ein, der dasjenige Subnetz angibt, dessen Stationen (und damit alle Stationen dieses Subnetzes) berechtigt sein sollen, das SNMP Setup zu ändern.

8.2.5 Ethernet-Schnittstelle

In Abhängigkeit von den Schnittstellentypen, die Ihr Access Point Radio Link-Modul anbietet, können Sie aus folgenden Optionen wählen (siehe Abbildung 42 Ethernet-Schnittstelle auswählen):

Abbildung 42 Ethernet-Schnittstelle auswählen



Weitere Informationen über die Auswahl der Ethernet-Schnittstelle finden Sie in der Online-Hilfe des RLM Manager-Programms.

8.3 Konfiguration großer Netzwerke

Jede Konfiguration der Radio Link-Module zeichnet sich durch zwei Parameter aus:

- Allgemeine Parameter, die auf ALLEN Radio Link-Modulen in Ihrem Netzwerk identisch sein müssen, und
- eindeutige Parameter, die nur ein und kein anderes Access Point RLM in Ihrem Netzwerk aufweisen darf.

In größeren Netzwerkumgebungen kann es unter Umständen sehr lästig sein, die allgemeinen Parameter auf jedes einzelne Radio Link-Modul zu kopieren, um im gesamten Netzwerk Konsistenz zu erreichen. Mit zunehmender Zahl der RLMs in einem Netzwerk steigt auch das Fehlerrisiko (z.B. als Ergebnis von Tippfehlern).

Inkonsistente Werte bei allgemeinen Parametern oder doppelte Werte bei eindeutigen Parametern können unvorhersehbare Auswirkungen auf die Leistungsfähigkeit Ihres Netzwerkes haben. Dokumentieren Sie detailliert die Einstellungen Ihres Netzwerks, um fehlerhafte Konfigurationen zu vermeiden.

Deshalb ist es ratsam, eine Vorlagendatei zu erstellen, die die Einstellungen für alle allgemeinen Parameter, die für jedes Access Point Radio Link-Modul innerhalb Ihres Netzwerks gültig sind, enthält.

8.3.1 Allgemeine Parameter

Allgemeine Parameter, wie zum Beispiel der Netzwerkname oder das SNMP-Kennwort für Lese und Lese-/Schreibvorgänge werden verwendet, um festzulegen, welche Radio Link-Module zur selben Netzwerkumgebung gehören. Sie sind das Unterscheidungsmerkmal, das Ihre RLM-Gruppe von einer anderen (benachbarten) Netzwerkumgebung trennt.

Eine Liste allgemeiner Parametern finden Sie in Tabelle 7 Allgemeine RLM-Parameter; diese Tabelle zeigt auch, welche mithilfe welcher Registerkarten des RLM Manager Sie diese Parameter anzeigen oder ändern können.

Tabelle 7 Allgemeine RLM-Parameter

Parameter	Registerkarte des RLM Manager
• Netzwerkname	Wireless Interfaces
• zu filternde Protokolle • MAC-Filterung	Bridge
• Subnetzmaske der Radio Link-Module • Standard-IP-Adresse des Router • Standard-TTL	Access Point IP
• Passwort für Lesevorgänge • Passwort für Lese-/ Schreibvorgänge • SNMP IP-Zugriffsliste • (Optional) Trap Host-IP-Adresse und Kennwort	SNMP

8.3.2 Eindeutige Parameter

Eindeutige Parameter (wie zum Beispiel die IP-Adresse oder der Systemname) werden verwendet, um die einzelnen Radio Link-Module innerhalb der RLM-Gruppe voneinander im Netzwerk unterscheiden zu können. Tabelle 8 Eindeutige RLM-Parameter führt die wichtigsten eindeutigen Parameter auf.

Tabelle 8 Eindeutige RLM-Parameter

Parameter	Menü im RLM Manager-Setup
• IP-Adresse der Radio Link-Module	Access Point IP
• Systemname • Systemstandort	SNMP

8.3.3 Konsistente Verwaltung des Systems

Eine große Anzahl Radio Link-Module lässt sich am einfachsten konsistent verwalten, indem man das erste Access Point Radio Link-Modul konfiguriert und diese Konfiguration in einer Datei speichert. Verwenden Sie diese Datei als Vorlage, die Sie in die anderen RLMs uploaden können.

Nachdem Sie die Vorlagendatei in jedes Radio Link-Modul geladen haben, können Sie die eindeutigen Parameter für jedes RLM festlegen, um die RLMs von den anderen Radio Link-Moduls in diesem Netzwerk unterscheiden zu können.

Mit anderen Worten, eine große Anzahl von Radio Link-Modulen können Sie am einfachsten verwalten, indem Sie:

1. Vorbereitung
   Alle notwendigen Informationen, die sich auf alle zu konfigurierenden Radio Link-Module beziehen, ermitteln und aufzeichnen,
2. Erstellung einer Vorlagendatei
   die allgemeinen Parameter, die für alle Radio Link-Module innerhalb Ihres Netzwerks gelten, ermitteln und einrichten.

3. Konfiguration aller Radio Link-Module
 die Vorlagendatei importieren und alle eindeutigen Parameter eingeben, um die Access Point Radio Link-Module innerhalb des Netzwerks voneinander unterscheiden zu können.



ACHTUNG:
Wir empfehlen, eine Sicherheitskopie der Konfiguration eines jeden Radio Link-Moduls zu erstellen. Verwenden Sie hierzu im Hauptfenster des RLM Manager die Option Download Config File. Wählen Sie den Dateinamen so, dass Sie einfach die Datei problemlos dem zugehörigen Radio Link-Modul zuordnen können.

8.3.3.1 Vorbereiten großangelegter Netzwerke

Sie müssen folgende Tätigkeiten ausführen, um die Konfiguration vorzubereiten:

- Entpacken Sie das Radio Link-Modul und tragen Sie, wie in diesem Dokument unter Startkonfiguration (Seite 260) beschrieben, dessen Seriennummer und MAC-Adresse im “Access Point Configuration Record” ein.
- Erstellen Sie eine Liste der in Ihrem Netzwerk verfügbaren IP-Adressen; für jedes Radio Link-Modul werden Sie eine eigene IP-Adresse benötigen.
- Verwenden Sie den “Access Point Configuration Record,” um jedem Ihrer RLMs eine IP-Adresse zuzuweisen.

- Dokumentieren Sie den geplanten Systemstandort eines jeden Radio Link-Moduls im “Access Point Configuration Record.”

8.3.3.2 Erstellung einer Vorlagendatei

1. Konfigurieren Sie das erste Radio Link-Modul und gehen Sie wie bereits unter Konfigurieren von Infrastruktur-Netzwerken (Seite 62) beschrieben vor, um eine Vorlagendatei zu erstellen.
2. Speichern Sie die Konfiguration dieses Radio Link-Moduls wie in Schritt 4 - Erstellen einer Sicherungsdatei der Konfiguration (Seite 72) beschrieben auf einer Diskette.
3. Erstellen Sie eine Kopie der gesicherten Datei und nennen Sie sie “common.cnf.” Sie können auch einen beliebigen anderen Namen verwenden. Nur sollten Sie anhand des Dateinamens sofort erkennen können, dass es sich hier um die Vorlage für die Konfiguration der anderen RLMs in Ihrem Netzwerk handelt.



ACHTUNG:
Verwenden Sie nicht Ihre ursprüngliche Sicherungskopie als Vorlagendatei. Jede Änderung an dieser Datei kann Ihnen die vollständige Wiederherstellung der Originalkonfiguration Ihres ersten RLMs erschweren, falls das System einmal ausfällt. Halten Sie immer Sicherheitskopien auf getrennten Datenträgern und/oder getrennten Aufbewahrungsorten bereit.

8.3.3.3 Konfiguration anderer Radio Link-Module

Nachdem Sie die Vorlagendatei erstellt haben, können Sie nun mit der (Neu-)Konfiguration der anderen Radio Link-Module im Batch-Modus beginnen. Dabei müssen Sie für jedes Access Point Radio Link-Modul wie folgt vorgehen:

- Starten Sie den RLM Manager und verbinden Sie sich mit dem Ziel-RLM.
- Uploaden Sie die Vorlagendatei, die die für alle Radio Link-Module gültigen Parameter enthält.
- Legen Sie die eindeutigen Parameter für jedes Access Point Radio Link-Modul fest.
- Sichern Sie die individuelle Konfiguration auf einer Diskette.

Gehen Sie hierbei im Detail wie folgt vor:

1. Starten Sie das RLM Manager-Programm.
2. Wählen Sie das gewünschte Radio Link-Modul aus der Liste, oder geben Sie eine spezifische IP-Adresse für ein Access Point Radio Link-Modul ein. Wird das gewünschte Access Point Radio Link-Modul nicht in der Liste angezeigt, wählen Sie aus dem RLM-Menü die Option **Refresh Radio Link Module List**.

   Falls das gewählte Access Point Radio Link-Modul immer noch die werksseitig vorgegebene IP-Adresse benutzt (wenn Sie zum Beispiel ein neues, gerade erst entpacktes Radio Link-Modul konfigurieren), werden Sie wie in Schritt 2 - Herstellen einer Verbindung zum Access Point RLM (Seite 64) beschrieben aufgefordert, eine Standard-IP-Adresse anzugeben.

3. Wechseln zu der Diskette und/oder zu dem Ordner, indem Sie die Vorlagendatei gespeichert haben, wenn Sie dazu aufgefordert werden.
4. Wählen Sie die Datei für die Konfigurationsvorlage (z.B. “common.cnf”), und klicken Sie auf die Schaltfläche **Open**.



WARNUNG:
Die IP-Adresse, die im Hauptfenster des RLM Manager in der Liste angezeigt worden war, wurde nun durch die IP-Adresse ersetzt, die in der Vorlagendatei angegeben war. Gehen Sie entsprechend der im Folgenden beschriebenen Schritte vor, um die IP-Adresse auf den gewünschten Wert zu ändern. Wenn Sie dies nicht tun, werden mehrere Radio Link-Module möglicherweise mit der gleichen IP-Adresse konfiguriert, was zu unvorhersehbaren Verhalten in Ihrem Netzwerk führen kann.

Der RLM Manager hat nun die Einstellungen, wie sie in der Vorlagendatei vorgegeben waren, geladen. Nun müssen Sie all diejenigen Parameter einrichten, die nur für dieses Access Point Radio Link-Modul gültig sein sollen (siehe Eindeutige Parameter (Seite 244)), bevor Sie die Konfiguration sichern und zum Hauptfenster des Radio Link-Moduls zurückkehren, indem Sie auf **OK** klicken.

5. Legen Sie die eindeutigen Parameter fest, die für dieses Access Point Radio Link-Modul gültig sind.

   Tabelle 8 Eindeutige RLM-Parameter listet alle eindeutigen Parameter auf, die Sie in jedem Falle angeben müssen.

6. Sichern Sie nun die Konfiguration Ihres Access Point Radio Link-Moduls, indem Sie auf **OK** klicken. Sie kehren nun zum Hauptfenster des Radio Link-Moduls zurück.

7. Erstellen Sie eine Sicherheitskopie der Konfigurationsdatei für dieses Access Point Radio Link-Modul, indem Sie im RLM-Menü die Option **Download Config File** auswählen.

   Wählen Sie den Dateinamen so, dass Sie einfach die Datei problemlos dem zugehörigen Radio Link-Modul zuordnen können.

Alle allgemeinen und eindeutigen Parameter werden nun dauerhaft in den nichtflüchtig FlashROM des Access Point Radio Link-Modul geladen. Sie sind im Radio Link-Modul gespeichert und bleiben selbst bei Ein- und Ausschalten des Geräts erhalten.

Wiederholen Sie die Schritte 2 - 7 für jedes andere Access Point Radio Link-Modul, das Sie konfigurieren.

8.3.3.4 Abschließen der Installation

Wenn Sie die Radio Link-Module an Ihrem Schreibtisch konfiguriert haben, wenn sich also die RLMs noch nicht an dem für Sie vorgesehenen Standort befanden, sollten Sie die Access Point Radio Link-Module für Ihre Technikern eindeutig etikettieren und eindeutige Installationsanweisungen zur Verfügung stellen.

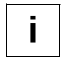
1. Notieren Sie für jedes Access Point Radio Link-Modul den vorgesehenen Standort auf einem Etikett und bringen Sie das Etikett auf dem Radio Link-Modul an.
2. Dokumentieren Sie den Namen der Datei, die die Konfiguration des RLM enthält, sowie den Standort, an dem das Access Point Radio Link-Modul installiert wird, im “Access Point Configuration Record.”
3. Verwahren Sie Ihre Sicherheitskopien (*.cnf), Ihre Vorlagendatei (**“**common.cnf”) und Ihren “Access Point Configuration Record” an einem sicheren Ort, sobald Sie alles abgeschlossen haben.

8.4 Ändern der Konfiguration

Sie können die Konfiguration des Access Point Radio Link-Moduls ändern, indem Sie im Hauptfenster des RLM Manager auf die Schaltfläche **Edit** klicken.

Bitte bedenken Sie, dass Sie das Radio Link-Modul mit Hilfe seiner neuen IP-Adresse und seines neuen Kennworts für Lese- und Lese-/Schreibvorgänge (falls sie den Parameter für das Kennwort für Lese-/Schreibvorgänge geändert haben) ansprechen müssen, um die Konfigurationsdatei zu öffnen. Falls es sich bei Ihrer SIMATIC NET IWL Management-Station um eine drahtlose Station handelt, müssen Sie unter Umständen die Schnittstellenparameter der Station ändern, damit die Werte wieder den ursprünglich im Access Point Radio Link-Modul gespeicherten Werten entsprechen.

Alternativ können Sie, falls Sie das Kennwort für den Lese-/Schreibzugriff oder irgend eine andere notwendige Einstellung vergessen haben, die werksseitigen Voreinstellungen wiederherstellen. Dies ist ausführlich in Abschnitt Erzwungener Neustart (Seite 275) beschrieben.



HINWEIS:

Wenn Sie an der Konfiguration eines bestimmten Radio Link-Moduls Änderungen vornehmen, sollten Sie Ihren “Access Point Configuration Record” aktualisieren, sodass er die neue Konfiguration widerspiegelt.

8.4.1 Ändern von allgemeinen Parameter

Wenn Sie Änderungen an den allgemeinen Parametern vornehmen müssen, also den Parametern, die für alle Radio Link-Module gütig sind, sollten Sie am besten folgendermaßen vorgehen:

1. Ändern Sie die allgemeinen Parameter auf einem Access Point RLM.
2. Sichern Sie die Änderungen in einer neuen Vorlagendatei (z.B. “common.cnf”)
3. Gehen Sie wie in Abschnitt Konfiguration anderer Radio Link-Module (Seite 248) beschrieben vor.

8.5 Wiederherstellen einer gesicherten Konfiguration

Gehen Sie folgendermaßen vor, um Konfigurationsdateien wiederherzustellen, die zuvor gesichert worden waren:

1. Starten Sie das RLM Manager-Programm.
2. Wählen Sie das Radio Link-Modul aus, in das Sie die Konfigurationsdatei einspielen möchten.
3. Wählen Sie im Access Point RLM-Menü die Option **Upload Config File**.
4. Wählen Sie die Konfigurationsdatei aus, die Sie hochladen wollen, und klicken Sie auf **Öffnen**.
5. Wenn Sie zur Bestätigung des Hochladens aufgefordert werden, prüfen Sie, ob das Meldungsfenster die korrekte IP-Adresse wiedergibt.
   - Ist die IP-Adresse korrekt, klicken Sie einfach auf **Yes**, um fortzufahren. Das Access Point Radio Link-Modul wird nun automatisch neu konfiguriert.
   - Klicken Sie auf **No**, wenn die IP-Adresse nicht korrekt ist, um zurückzukehren und den Hochladevorgang abzubrechen.

Die neuen Parametereinstellungen werden nun in den FlashRom des Radio Link-Moduls geladen. Dies bedeutet, dass die Parameter erhalten bleiben, selbst wenn das Gerät aus- und eingeschalten wird. Um die Parameter nochmals zu ändern und Ihre Radio Link-Module nochmals neu zu konfigurieren, wiederholen Sie einfach die in diesem Abschnitt beschriebenen Schritte.

8.6 Duale PC Card Konfiguration

Der Einsatz von zwei PC Card CP 1515 in einem RLM kann unterschiedlichen Zwecken dienen, z.B.:

- Verdopplung der Kapazität der Radio Link-Module.

Setzt man eine zweite PC Card in den zweiten Slot des Access Point Radio Link-Moduls, verdoppelt sich die Kapazität des Access Point RLM. Diese Option kann sich in IWL-Netzen als hilfreich erweisen, in denen ein hoher Anteil verlorener Telegramme einen schnellen Datenaustausch verhindert.

8.7 Über IP-Adressen und Subnetze

In größeren Organisationen, die zur Kommunikation IP-Adressen verwenden, beinhaltet die Netzwerkarchitektur unter Umständen unterschiedliche Netzwerksegmente (Subnetze), die üblicherweise durch einen Router oder ein Gateway von einander getrennt sind.

Wenn Sie die SIMATIC NET IWL-Infrastruktur in eine solche Netzwerkarchitektur installieren, müssen Sie darauf achten, dass alle Radio Link-Module und alle drahtlosen Stationen innerhalb des selben Subnetz installiert sind, z.B. auf der selben Seite des Routers oder des Gateways.

Die Roaming-Funktionalität funktioniert nicht über Router hinaus. Wenn Radio Link-Module mit unterschiedlichen Subnetzen verbunden sind, kann eine mobile Station möglicherweise seine Netzwerkverbindung verlieren, wenn sie physikalisch in einen Bereich eintritt, in dem die RLMs mit einem anderen Subnetz verbunden sind.

Die Konfiguration und Verwaltung Ihrer Radio Link-Module erfolgt über den TCP/IP-Protokollstapel. Dies bedeutet, dass jedes Access Point RLM und Computer, den Sie konfigurieren möchten, über eine eindeutige IP-Adresse verfügen muss.

Dabei wird, wie bereits in diesem Kapitel beschrieben, empfohlen, den Radio Link-Modulen "statische" IP-Adressen zuzuweisen. Dies gewährleistet, dass die RLMs an spezifischen Standorten immer über die gleiche IP-Adresse verfügen. Für die LAN-Administratorstationen können Sie entweder statische oder dynamische IP-Adressen, die von einem BOOTP- oder DHCP-Server vergeben werden, verwenden.

Wenn Sie LAN-Administratorstationen IP-Adressen zuweisen, stellen Sie bitte sicher, dass:

- jedes Gerät eine eindeutige IP-Adresse besitzt.
- alle Geräte dieselbe Subnetzmaske verwenden.



HINWEIS:

Das drahtlose Netzwerksystem benötigt keine IP-Adressen, um normale drahtlose Stationen mit den Netzwerk zu verbinden. Die Infrastruktur ist nur das “physikalische” Mittel, um einen Computer mit einem Radio Link-Modul zu verbinden, so wie Sie einen Draht verwenden könnten, um ihn mit einer Ethernet-Infrastruktur zu verbinden.

In Umgebungen, in denen das Betriebssystem das TCP/IP-Protokoll verwendet, benötigen Stationen jedoch unter Umständen eine IP-Adresse, um spezifische Netzwerkdienste (wie beispielsweise den Zugang zum Internet) nutzen zu können.

8.7.1 BOOTP und DHCP

Beim ersten Einschalten sendet das Access Point Radio Link-Modul eine Anforderung nach einer IP-Adresse aus. Falls in Ihrem Netzwerk ein BOOTP- oder DHCP-Server vorhanden ist, wird dieser Server dem Access Point Radio Link-Modul eine verfügbare IP-Adresse zuweisen.

In Abhängigkeit von den Einstellungen Ihres BOOTP- oder DHCP-Servers ist es unter Umständen erforderlich, dass Sie Ihrem BOOTP- oder DHCP-Server die MAC-Adresse des Radio Link-Moduls zuvor mitteilen. Weitere Informationen erhalten Sie in der Dokumentation Ihrer BOOTP/DHCP-Software.

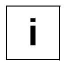
Eine von einem DHCP-Server zugewiesene IP-Adresse wird im flüchtigen Speicher des Access Point Radio Link-Moduls gespeichert. Wird das RLM beispielsweise neu gestartet, kann der DHCP-Server eine neue IP-Adresse zuweisen. Um größtmögliche Konsistenz zu gewährleisten, wird empfohlen, mithilfe des Felds **Access Point IP Address** auf der Registerkarte **Access Point IP** jedem Radio Link-Modul eine statische IP-Adressen zuzuweisen.

Wenn ein BOOTP-Server eine IP-Adresse zuweist, speichert er sie in einer eigenen Konfigurationsdatei. Diese Konfigurationsdatei enthält eine statische Eins-zu-eins-Zuweisung von MAC-Adresse zu IP-Adresse. Wenn ein BOOTP-Server verwendet wird und das Radio Link-Modul neu gestartet wird, ist die neue IP-Adresse des RLM identisch mit der IP-Adresse, die das Radio Link-Modul vor dem Neustart besaß.

A Startkonfiguration

A.1 Einführung

Das Radio Link-Modul ist mit einer werkseitig vorinstallierten Betriebssoftware ausgestattet. Neben dieser Software ist auf dem RLM auch eine werkseitig eingestellte Konfiguration geladen, die einen unmittelbaren Einsatz des Geräts “Out-of-the-Box” erlaubt.



HINWEIS:

Die werkseitig eingestellte Konfiguration sollte nicht mit einer "Standardkonfiguration" verwechselt werden. Wenn Sie beispielsweise einen Neustart- oder erzwungenen Neustart-Vorgang (weiter hinten in diesem Handbuch beschrieben) ausführen, kehrt das Gerät NICHT zur "werkseitig eingestellten" Konfiguration zurück.

Um eine Verbindung zum Radio Link-Modul herstellen zu können, müssen die Netzwerkparameter der einzelnen drahtlosen Stationen auf die Werte eingestellt werden, die auch für das RLM-Gerät festgelegt wurden.

- Wenn das Radio Link-Modul erstmals eingeschaltet wird, müssen diese Werte mit den Werten übereinstimmen, die in Tabelle 9 Startkonfiguration - RLM aufgeführt sind.
- Für den normalen Betrieb müssen diese Werte mit den Werten übereinstimmen, die Sie beim Konfigurieren des RLM-Geräts angegeben haben. Es empfiehlt sich, diese Informationen auf dem Formular "Access Point Configuration Record" in diesem Anhang zu notieren.

A.2 Werkseitig eingestellte Konfiguration

Tabelle 9 Startkonfiguration - RLM

RLM-Parameter		
Registerkarte "Access Point IP"	Option "Obtain an IP address from DHCP server"	Aktiviert
	Option "Default TTL"	64
Registerkarte "SNMP"	Option "Read Password"	public
	Option "Read/Write Password"	public
	Option "System Name"	xx-xx-xx-xx-xx-xx [1]
	Option "Trap Host IP address"	0.0.0.0 [2]
	Option "Trap Host Password"	public
	Option "SNMP IP Access List"	<All will be permitted>
Registerkarte "Bridge"	Option "Protocols to Filter"	<none>
	Option "Static MAC address Filter"	<none>
	Option "Spanning Tree"	Deaktiviert
	Option "Storm Thresholds"	Deaktiviert

Registerkarte "Access Control"	Option "(Static) Access Control"	<All will be permitted>
	Option "RADIUS Server Access Control"	Deaktiviert
Registerkarte "Link Integrity"	Option "Link Integrity"	Deaktiviert

1. Ethernet-MAC-Adresse des Geräts (auf einem kleinen Etikett auf dem Prozessormodul aufgedruckt).

2. Es werden keine SNMP-Trap-Nachrichten mit dieser IP-Adresse gesendet.

Werkseitig eingestellte Konfiguration

Tabelle 10 Startkonfiguration - Schnittstelle

Drahtlose Schnittstelle		
	Netzwerkname	WaveLAN-Netzwerk
	RF-Kanal	2,462 MHz
	Option "Closed wireless system"	Deaktiviert
	Verschlüsselung	Deaktiviert
	Medienreservierung	Deaktiviert
	Unterstützung für Interferenzschutz	Deaktiviert
	DTIM-Periode	1
	Abstand zwischen APs	Groß
	Multicast-Geschwindigkeit	2 MBit/s

Access Point Configuration Record

Common Parameters

Wireless Network

Network Name: ____________________

Access Control

Access Control ❑ Enabled
Table File Name: ____________________
RADIUS server ❑ Enabled

SNMP

System Location: ____________________
IP Subnet Mask: ____________________
Read Password: ____________________
Read/Write Password: ____________________

Access Point Unique Identifiers

Serial Number	MAC Address	IP Address	IF	Frequency	Device Location	Date Installed	Configuration File
			❑E ❑A ❑B				
			❑E ❑A ❑B				
			❑E ❑A ❑B				
			❑E ❑A ❑B				
			❑E ❑A ❑B				
			❑E ❑A ❑B				
			❑E ❑A ❑B				
			❑E ❑A ❑B				
			❑E ❑A ❑B				

B Problembehandlung

B.1 Einführung

Beim Betrieb von drahtlosen LAN-Netzwerken auftretende Probleme können auf Folgendes zurückzuführen sein:

- Konfigurationskonflikte
- Komponentenfehler
- Probleme in herkömmlichen und drahtlosen Netzwerken

B.2 Vorgehensweise bei der Problembehandlung

Wenn Sie Konfigurationskonflikte beheben möchten, müssen Sie die Einstellungen der Konfigurationsparameter der betroffenen RLMs und Stationen vergleichen.

Um Komponentenfehler festzustellen, müssen Sie die LED-Aktivität des Radio Link-Moduls überprüfen. Sie können anhand der LED-Fehlertabelle ermitteln, ob das Problem auf einen Hardwarefehler (Komponentenfehler) zurückzuführen ist. Diese Tabelle bietet Ihnen auch Unterstützung beim Diagnostizieren und Beheben von Betriebsproblemen, die andere mögliche Ursachen haben.

Wenn das RLM scheinbar nicht mehr auf normale Bridging-Anforderungen reagiert, können Sie versuchen, das Gerät, wie unter Neustarten von RLMs beschrieben, neu zu starten. In außergewöhnlichen Fällen können Sie auch einen erzwungenen Neustart, wie im Abschnitt Erzwungener Neustart beschrieben, vornehmen.

Tabelle 11 LED-Fehlertabelle

Versor-gungs-spannung	Ethernet	Drahtlose Schnitt-stelle A	Drahtlose Schnitt-stelle B	Beschreibung/Maßnahme:
		A	B	
Dauer- grün	Grün blinkend	Grün blinkend	Grün blinkend	Normaler Betrieb, bei dem Blinken die Schnittstellenaktivität anzeigt. Keine Maßnahmen erforderlich.
	Aus	Aus	Aus	Normaler Betrieb, bei dem keine LAN-Aktivität angezeigt wird. • Keine Maßnahmen erforderlich. • (Optional) Überprüfen Sie, ob alle Ethernetverbindungen ordnungsgemäß installiert sind.

<table>
<tr><td>Aus</td><td>Aus</td><td>Aus</td><td>Aus</td><td>Keine Stromversorgung.
• Überprüfen Sie das Netzkabel.
• Überprüfen Sie das Netzteil.</td></tr>
<tr><td rowspan="3">Dauer- grün</td><td rowspan="2">Grün blinkend</td><td>Amber</td><td>-</td><td rowspan="3">Netzwerküberlastung
Die Ethernetverbindung sendet mehr Datenverkehr an die drahtlosen Stationen, als die RLM-Brücke an die Schnittstelle weiterleiten kann[1].
Führen Sie die Remote-Statistik-Funktion von RLM Manager aus, um die Netzwerkleistung zu überprüfen.
Eliminieren Sie redundanten Verkehr durch:
• Filtern der Protokolle
• Festlegen des Storm-Schwellenwerts, oder
• Herunterfahren von Ethernet-Stationen mit übermäßiger Datenübertragung</td></tr>
<tr><td>-</td><td>Amber</td></tr>
<tr><td>Grün</td><td>Amber</td><td>Amber</td></tr>
</table>

1. Wenn die Verkehrslast die drahtlose Durchsatzkapazität (>11 MB/s) überschreitet, puffert das RLM diese Anforderungen. In dieser Situation ist der Puffer jedoch voll, und die Pakete werden ignoriert.

Versorgungsspannung	Ethernet	Drahtlose Schnittstelle A	Drahtlose Schnittstelle B	Beschreibung/Maßnahme:
Ⓘ	•—•	∿ A	∿ B	
Dauergrün	Rot blinkend	-		Frames werden aus unbekanntem Grund abgewiesen. • Führen Sie die Remote-Statistik-Funktion von RLM Manager aus, um die Anzahl der fehlerhaften Pakete zu überprüfen. • Wenn die Anzahl hoch ist, führen Sie einen Remote Link-Test aus, um die Station zu ermitteln, die den Paketverlust verursacht.
	-	Rot blinkend		
		-		
Gelb	Aus	Aus	Aus	Erzwungener Neustart-Status. • Fahren Sie mit dem Verfahren für den erzwungenen Neustart, wie in Anhang C “Erzwungener Neustart” in diesem Benutzerhandbuch beschrieben, fort.
	Gelb	Gelb	Gelb	

Gelb	Grün blinkend	Aus	Aus	Erzwungener Neustart-Status. Die blinkende LED zeigt LAN-Aktivität auf der jeweiligen LAN-Schnittstelle an. Diese Aktivität wird in der Regel durch die LAN-Administratorstation verursacht, die einen erzwungenen Neustart ausführt. • Fahren Sie mit dem Verfahren für den erzwungenen Neustart, wie in Anhang C "Erzwungener Neustart" in diesem Benutzerhandbuch beschrieben, fort.
	Aus	Grün blinkend	Aus	
		Aus	Grün blinkend	
Rot	-	-	-	Allgemeiner Hardwarefehler • Starten Sie das RLM, wie in diesem Anhang beschrieben, neu. • Wenden Sie sich an den technischen Support von Siemens, falls das Problem weiterhin besteht.

-	Gelb	-	-	Ethernet-Hardwarefehler • Starten Sie das RLM, wie in diesem Anhang beschrieben, neu. • Wenden Sie sich an den technischen Support von Siemens, falls das Problem weiterhin besteht.
	-	Gelb	-	SIMATIC NET IWL-Hardwarefehler • Starten Sie das RLM, wie in diesem Anhang beschrieben, neu. • Wenden Sie sich an den technischen Support von Siemens, falls das Problem weiterhin besteht.
		-	Gelb	
			Aus	Falls die CP 1515-Karte beschädigt ist, was durch Einsetzen der Karte in den SIMATIC NET IWL-Computer überprüft werden kann, sollten Sie die Karte an den autorisierten Fachhändler zurückgeben.
			Gelb	

B.3 Neustarten von RLMs

Wenn ein bestimmtes Radio Link-Modul nicht mehr auf normale Bridging-Anforderungen reagiert, können Sie das Access Point RLM neu starten (zurücksetzen). Sie können die RLMs entweder unmittelbar manuell oder von einem Remote-Standort aus neu starten.

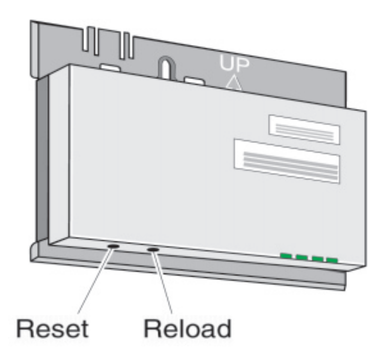
Beim Neustart führt das Radio Link-Modul eine Startdiagnose aus und startet den Bridging-Vorgang anhand der Konfigurationsparameter, die vor dem Neustart auf dem RLM gespeichert wurden. Bei RLMs mit werksseitigen Standardeinstellungen lauten diese Parameter wie in Tabelle 9 Startkonfiguration - RLM angegeben.

B.3.1 Manueller Neustart

Gehen Sie wie folgt vor, um das RLM manuell neu zu starten:

1. Nehmen Sie die Abdeckung des Radio Link-Moduls ab. Hinweise hierzu finden Sie im Handbuch “Industrial Wireless LAN, Radio Link Module RLM” auf der Industrial Wireless LAN CD, die im Lieferumfang des RLM enthalten ist.
2. Suchen Sie die beiden kleinen Vertiefungen auf der Unterseite des Prozessormoduls, die mit "Reset" und "Reload" gekennzeichnet sind (siehe Abbildung 43 Reset-Taste).

Abbildung 43 Reset-Taste



3. Verwenden Sie einen spitzen Gegenstand, wie beispielsweise die Spitze eines Kugelschreibers, um die **Reset**-Taste zu drücken.

   Das RLM wird neu gestartet und führt die Startdiagnose aus. Dies wird durch einen farblichen Wechsel der LED-Anzeigen von Rot über Gelb nach Grün angezeigt.

4. Wenn die LED der Betriebsanzeige grün leuchtet und die anderen LEDs aus sind oder blinken (Anzeige für die LAN-Aktivität), können Sie die Abdeckung des RLM wieder aufsetzen.

Nach etwa 15 Sekunden startet das Gerät den Bridging-Vorgang anhand der Konfigurationsparameter, die vor dem Neustart auf dem RLM gespeichert wurden.

B.3.2 Neustart von einem Remote-Standort

So starten Sie das Radio Link-Modul von einem Remote-Standort:

1. Starten Sie die Anwendung RLM Manager.
2. Wählen Sie das Ziel-Acess Point RLM in der Liste aus, oder geben Sie die IP-Adresse für ein bestimmtes RLM ein.
3. Öffnen Sie das RLM-Menü.
4. Wählen Sie **Reboot** RLM.

   Der RLM Manager fordert Sie nun zur Eingabe des zum Neustarten des Geräts erforderlichen Kennworts auf.
5. Geben Sie das Kennwort für Lese-/Schreibvorgänge ein, und klicken Sie auf **OK**.
6. Das Radio Link-Modul startet neu und führt die Startdiagnose aus.

Nach etwa 15 Sekunden startet das RLM den Bridging-Vorgang anhand der Konfigurationsparameter, die vor dem Neustart auf dem RLM gespeichert wurden.

Wenn Sie die Konfigurationsdatei anzeigen oder die Leistung des Radio Link-Moduls nach einem Neustart überwachen möchten, müssen Sie eventuell warten, bis das Gerät die Startdiagnose abgeschlossen hat, bevor Sie erneut auf das Access Point RLM zugreifen können.

C Erzwungener Neustart

C.1 Einführung

Mit Hilfe eines erzwungenen Neustarts können Sie die Wiederherstellung in den folgenden Situationen vornehmen:

- Wenn das Radio Link-Modul dem System nicht mehr antwortet.
- Wenn Sie eindeutige Kennungen, wie die IP-Adresse, das SNMP-Kennwort für Lese-/Schreibvorgänge oder andere Parameter geändert haben, die die Kommunikation mit dem RLM verhindern.
- Wenn das Access Point RLM mit falschen Netzwerkparametern konfiguriert wurde, die den Zugriff auf das RLM über die Netzwerkschnittstelle verhindern.



ACHTUNG:
Wenn Sie einen erzwungenen Neustart durchführen müssen, sollten Sie Folgendes berücksichtigen:

a. Auf die Radio Link-Module mit Netzwerkschnittstellen, die auf den Modus für den erzwungenen Neustart eingestellt sind, kann nicht über die SIMATIC NET IWL-Netzwerkschnittstelle zugegriffen werden.

b. Der erzwungene Neustart darf nur bei jeweils einem Radio Link-Modul ausgeführt werden.

Es könnte sonst zu unerwarteten Administrationsproblemen kommen, weil mehrere Geräte mit identischem Konfigurationsabbild und identischer IP-Adresse konfiguriert werden.

Im erzwungenen Neustart-Modus beendet das RLM den Bridging-Vorgang. Das Access Point RLM akzeptiert nur das Laden eines neuen Softwareabbilds in das FlashROM.

Um im erzwungenen Neustart-Modus auf das Radio Link-Modul zugreifen zu können, müssen Sie möglicherweise die LAN-Administratorstation neu konfigurieren.

Wenn Ihr RLM mit CP 1515-Karten ausgerüstet ist, können Sie den erzwungenen Neustart anhand eines Konfigurationsszenarios ausführen, das unter Einrichten der LAN-Administratorstation (siehe Abbildung 6 Leitungsgebundener Zugang über eine Netzwerkverbindung oder Abbildung 8 Drahtloser Zugang über eine indirekte Verbindung) beschrieben ist.

C.2 Ausführen eines erzwungenen Neustarts

Das Verfahren für den erzwungenen Neustart besteht aus drei Schritten:

Schritt 1 - Vorbereitungen.

Schritt 2 - Modus für den erzwungenen Neustart initiieren.

Schritt 3 - Konfigurieren und Laden von Dateien.

Der vierte Schritt ist zwar optional, wird jedoch empfohlen:

Schritt 4 - Erstellen einer Sicherungskopie

C.2.1 Schritt 1 - Vorbereitungen

Der erzwungene Neustart kann nur ausgeführt werden, wenn Sie physikalischen Zugriff auf das RLM haben.

- Machen Sie sich mit dem Standort des RLMs vertraut:
  Benötigen Sie zusätzliche Hilfsmittel für den Zugang zum Access Point RLM, wie beispielsweise eine Leiter oder die Schlüssel zu dem Raum, in dem sich das Radio Link-Modul befindet?
- Besitzen Sie eine Sicherungskopie der aktuellen Konfigurationsdatei (*.cnf) des RLM?
  - Wenn **Ja**, dann können Sie die ursprüngliche Konfiguration anhand der Sicherungskopie wiederherstellen.
  - Wenn **Nein**, dann müssen Sie alle benutzerdefinierten Parameter für das RLM, die in Ihrem Netzwerk zutreffen, erneut einstellen.

Sicherungskopien wurden möglicherweise bei der Erstinstallation anhand der Option **Download Config File** der Anwendung RLM Manager erstellt.

- Wenn Sie Zugang zur Website von Siemens **http://www.siemens.com/mobic** haben, können Sie die neueste Firmware (*.bin) für das Radio Link-Modul herunterladen.
- Es empfiehlt sich, eine temporäre IP-Adresse für das Access Point RLM anzugeben. So geben Sie diese temporäre IP-Adresse ein:
  - Starten Sie die Anwendung RLM Manager.
  - Wählen Sie die Option **Options** im Menü **Tools**.
  - Geben Sie die temporäre IP-Adresse im Feld **Local IP address** ein.

  Die temporäre IP-Adresse wird dem Radio Link-Modul im erzwungenen Neustart-Modus zugewiesen. Dies erfolgt, um die Konfiguration und das Laden der Softwaredatei zu ermöglichen, bis das Radio Link-Modul über eine endgültige IP-Adresse verfügt.

Es gibt zwei Konfigurationsmöglichkeiten für die LAN-Administratorstation, um den logischen Zugriff auf das RLM zu ermöglichen:

- Die LAN-Administratorstation ist die SIMATIC NET IWL-Station.
- Die LAN-Administratorstation ist eine herkömmliche Station (Ethernet-Station).

C.2.1.1 Die LAN-Administratorstation ist eine herkömmliche Station

Die LAN-Administratorstation ist über die Ethernet-Schnittstelle des RLMs mit dem RLM verbunden.

- Stellen Sie sicher, dass die LAN-Administratorstation und das RLM an das gleiche LAN-Segment (Subnetz) angeschlossen sind.

  Um die Kommunikation mit dem RLM im erzwungenen Neustart-Modus zu ermöglichen, sind zwischen dem Ziel-RLM und der LAN-Administratorstation keine Router zulässig.
- Wenn Sie die IP-Adressierung verwenden, sollten Sie die IP-Adresse notieren, die vom Radio Link-Modul verwendet werden soll.

C.2.1.2 Die LAN-Administratorstation ist eine drahtlose Station

Sie können eine drahtlose LAN-Administratorstation **NUR** zum Zugreifen auf das Radio Link-Modul im Modus für den erzwungenen Neustart verwenden, wenn die Station indirekten Zugriff auf das RLM hat, wie unter Drahtloser Zugang über eine indirekte Verbindung (Seite 56) beschrieben.

Stellen Sie sicher, dass die Einstellungen der LAN-Administratorstation mit den Einstellungen des RLMs übereinstimmen, zu dem Sie die Verbindung im erzwungenen Neustart-Modus herstellen möchten.

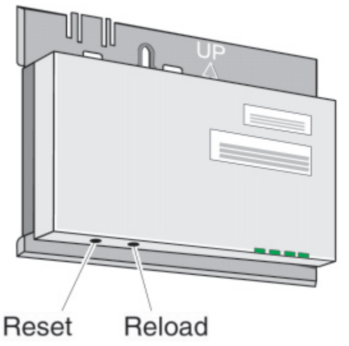
- Vergewissern Sie sich, dass die LAN-Administratorstation in Reichweite des RLM befindet.

Wenn Sie die IP-Adressierung verwenden, sollten Sie die (neue) IP-Adresse notieren, die Sie dem Radio Link-Modul im erzwungenen Neustart-Modus zuweisen möchten.

C.2.2 Schritt 2 - Modus für den erzwungenen Neustart initiieren

1. Entfernen Sie die Abdeckung vom Radio Link-Modul.
2. Suchen Sie die beiden kleinen Vertiefungen auf der Unterseite des Prozessormoduls, die mit "Reset" und "Reload" gekennzeichnet sind (siehe Abbildung 44).

Abbildung 44 Reset- und Reload-Taste



3. Verwenden Sie einen spitzen Gegenstand, wie beispielsweise die Spitze eines Kugelschreibers, um die **Reset**-Taste zu drücken.
4. Lassen Sie die **Reset**-Taste los, und warten Sie 5 Sekunden.

Das RLM führt die Startdiagnose aus. Dies wird durch LED-Aktivität und einen farblichen Wechsel der LED-Anzeigeleuchten von Gelb über Rot nach Grün angezeigt.

5. Drücken Sie nach etwa 5 Sekunden mit Hilfe des spitzen Gegenstandes die **Reload**-Taste, und halten Sie sie ungefähr 30 Sekunden gedrückt.

   Es erfolgt erneut ein farblicher Wechsel der LED-Anzeigeleuchten von Gelb über Rot nach Grün.

6. Lassen Sie die **Reload**-Taste los, sobald alle LEDs in der Farbe Gelb aufleuchten.

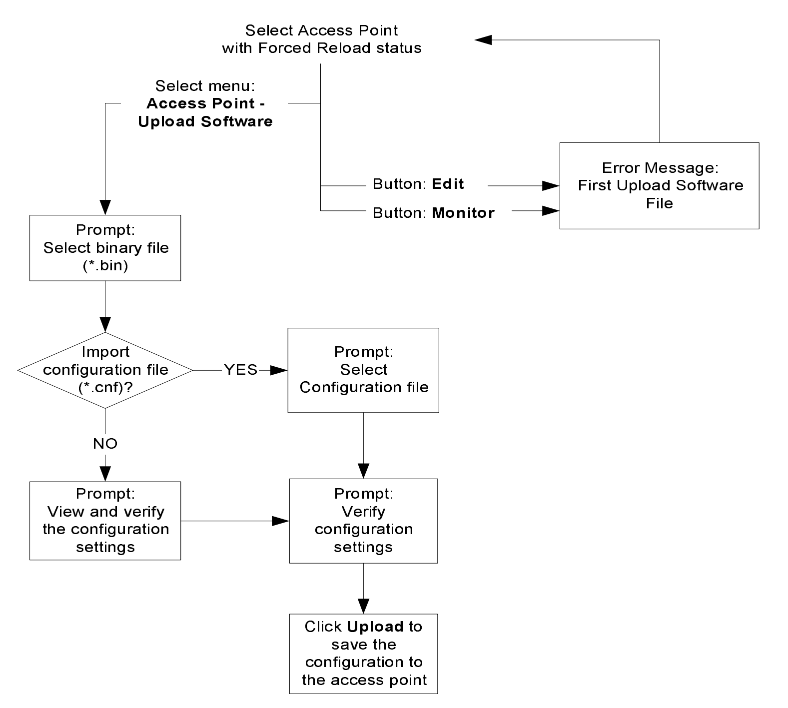
   Die LED der Betriebsanzeige leuchtet in Gelb. Andere LEDs sind möglicherweise aus oder blinken grün, um die LAN-Aktivität der dazugehörigen Schnittstelle anzuzeigen.

7. Starten Sie die Anwendung RLM Manager, und fahren Sie mit “Schritt 3 - Konfigurieren und Laden von Dateien” fort.

C.2.3 Schritt 3 - Konfigurieren und Laden von Dateien

Der vollständige Ablauf der Konfiguration und des Ladens der Dateien beim erzwungenen Neustart ist in Abbildung 45 veranschaulicht.

Abbildung 45 Konfiguration des Ladevorgangs beim erzwungenen Neustart



Gehen Sie wie folgt vor, um das Radio Link-Modul im erzwungenen Neustart-Modus zu konfigurieren und die Konfiguration zu laden:

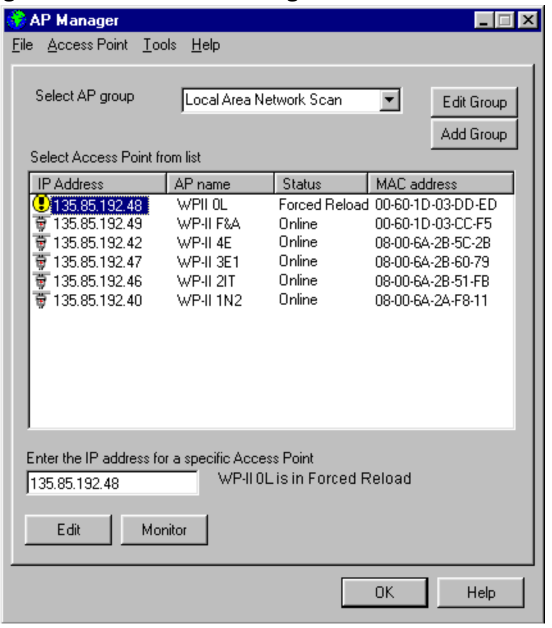
1. Wählen Sie das RLM aus, das sich im erzwungenen Neustart-Modus befindet.

   Das Radio Link-Modul im erzwungenen Neustart-Modus wird im Hauptfenster des RLM Manager oben in der Liste angezeigt und ist wie folgt zu erkennen (siehe Abbildung 46):

   - Das RLM ist mit dem Symbol für den erzwungenen Neustart markiert.
   - Das RLM ist mit der Statusangabe "Forced Reload" markiert.
   - Die IP-Adresse des RLM lautet 153.69.254.254.

Ausführen eines erzwungenen Neustarts

Abbildung 46 Das RLM im erzwungenen Neustart-Modus



2. Wählen Sie im Menü "Access Point" des RLM Managers die Option **Upload Firmware**, um die Konfiguration und den Ladevorgang zu starten.
   - Wenn Sie vor dem Laden der Firmware auf die Schaltfläche **Edit** oder **Monitor** klicken, werden Sie dazu aufgefordert, zunächst die Firmware zu laden.
3. Wechseln Sie im Fenster **Öffnen** zum Installationsverzeichnis der Anwendung RLM Manager. Wenn Sie die neueste RLM-Firmware von der Siemens SIMATIC NET IWL-Website heruntergeladen haben, wählen Sie das Verzeichnis, in dem Sie die heruntergeladene Datei gespeichert haben.
4. Wählen Sie in der Liste der angezeigten Dateien die Datei "wpnt*xxx*.bin", (wobei "*xxx*" für die Version der RLM-Firmware steht).
5. Klicken Sie auf die Schaltfläche **Open**, um die Firmwaredatei zu öffnen.
6. Sie können nun eine Sicherungskopie der Konfigurationsdatei auf das Radio Link-Modul laden.



HINWEIS:

Wenn Sie eine Konfigurationsdatei importieren, sollten Sie sicherstellen, dass Sie die richtige Sicherungsdatei importieren. Falls Sie das Radio Link-Modul mit einer Konfigurationsdatei konfigurieren, die mit der Konfiguration eines anderen Radio Link-Moduls identisch ist, kann dies zu unvorhersehbaren Verhalten in Ihrem Netzwerk führen.

Ausführen eines erzwungenen Neustarts

- Wenn Sie eine Sicherungskopie der Konfigurationsdatei **besitzen**, und wenn Sie die Datei zum Konfigurieren des Radio Link-Moduls **verwenden** möchten, klicken Sie auf **Yes**.

  Wählen Sie die Sicherungskonfigurationsdatei (*.cnf), und klicken Sie auf **Open**, um die Sicherungdatei der Konfigurationseinstellungen zu öffnen.

  Es empfiehlt sich, die Konfigurationseinstellungen zu überprüfen. Klicken Sie auf **OK**, um den Vorgang fortzusetzen.

- Wenn Sie **nicht** über eine Sicherungskopie der Konfigurationsdatei verfügen, oder wenn Sie über eine Datei verfügen, diese Datei jedoch **nicht** zum Konfigurieren des RLM verwenden möchten, klicken Sie auf **No**.

  Sie sollten in diesem Fall die Konfigurationseinstellungen des Access Point RLM nun manuell ändern/überprüfen (d.h. eine eindeutige IP-Adresse zuweisen, die Parameter und (gegebenenfalls) die anderen Access Point RLM-Kennungen, wie die IP-Adresse und die SNMP-Kennwörter, festlegen).

7. Das Fenster "Edit Configuration" wird angezeigt. Beachten Sie, dass im Fenster "Edit Configuration" statt der Schaltfläche **OK** die Schaltfläche **Upload** zum Laden der Konfigurationseinstellungen auf das RLM erscheint. Dies bedeutet, dass Sie eine lokale Konfigurationsdatei bearbeiten und noch nicht mit dem RLM verbunden sind.
8. Prüfen Sie die Konfigurationseinstellungen auf sämtlichen Registerkarten und ändern Sie die Einstellungen ggf.
   Informationen zum Ändern der Konfigurationseinstellungen finden Sie unter Einfache Netzkonfigurationen (Seite 59).

9. Klicken Sie auf die Schaltfläche **Upload**, um die neuen Konfigurationseinstellungen im erzwungenen Neustart-Modus auf das Access Point RLM zu laden.

   Die Meldung "Please wait while trying to connect to the RLM" erscheint. Während versucht wird, eine Verbindung zum Radio Link-Modul herzustellen, wird ein Ping-Befehl an die IP-Adresse gesendet, die in den Konfigurationseinstellungen angegeben ist.

   - Falls die in der Konfiguration angegebene IP-Adresse bereits existiert, werden Sie zur Eingabe einer neuen IP-Adresse aufgefordert. Wenn die IP-Adresse noch nicht existiert, wird der Ladevorgang fortgesetzt.
   - Da das Kennwort des RLM im erzwungenen Neustart-Modus immer "public" lautet, müssen Sie dieses Kennwort vor dem Laden von Informationen auf das Access Point RLM nicht eingeben.

10. Wenn Sie zum Bestätigen des Neustarts des Remote-Systems aufgefordert werden, klicken Sie auf **Yes**, um den Vorgang fortzusetzen.

    Die lokale Firmwaredatei ("wpntxxx.bin") importiert nun die Konfigurationseinstellungen und speichert sie. Weitere Informationen finden Sie unter Funktionsweise des Ladevorgangs (Seite 294).

    Wenn Sie die ursprüngliche Softwaredatei sichern möchten, sollten Sie eine Sicherungskopie dieser Datei erstellen.

11. Sie werden erneut zum Bestätigen des Neustarts des Remote-Systems aufgefordert. Prüfen Sie die Liste der angezeigten Parameter genau, um sicherzustellen, dass alle Einstellungen korrekt sind.

- Wenn im Popup-Fenster nicht die richtige IP-Adresse und/oder die richtigen SNMP-Kennwörter erscheinen, klicken Sie auf **No**, um den Vorgang abzubrechen.
- Wenn die IP-Adresse und/oder die SNMP-Kennwörter korrekt sind, klicken Sie auf **Yes**, um den Vorgang fortzusetzen.

12. Die Anwendung RLM Manager lädt nun die neue (wiederhergestellte) Konfiguration auf Ihr RLM und lädt sie in das FlashROM. Das RLM wird neu gestartet und beginnt den Bridging-Vorgang in ca. 60 Sekunden.

C.2.4 Erstellen einer Sicherungskopie

Es empfiehlt sich, die Konfigurationsparameter des Radio Link-Moduls in einer Sicherungsdatei (*.cnf) zu speichern. Erstellen Sie die Sicherungsdatei mit Hilfe der Option **Download Config File** im RLM-Menü.

Sie sollten die Konfigurationsdatei sichern um sie ggf. verwenden zu können für z.B. die Behebung von Netzproblemen mit der Funktion "erzwungener Neustart."

Speichern Sie die Sicherungsdatei mit einem Namen, der Aufschluss über ihren Inhalt gibt.

C.2.5 Startdiagnose

Beim Neustart führt das RLM eine Startdiagnose aus. Dies wird durch einen farblichen Wechsel der LED-Anzeigeleuchten von Gelb über Rot nach Grün angezeigt.

Die Startdiagnose dauert ungefähr 15 Sekunden. Nach Abschluss der Diagnose beginnt das RLM den Bridging-Vorgang. Dies wird durch die LED-Aktivität angezeigt. Weitere Informationen finden Sie unter Problembehandlung (Seite 266).

D Aktualisieren der RLM-Software

D.1 Informationen zur RLM-Software

Das Access Point RLM arbeitet mit eingebetteter Software, die auch als "Firmware" oder "Bridge-Kernel" bezeichnet wird. Diese Software ist bereits werkseitig vorinstalliert, so dass Sie sich normalerweise nicht mit der Software des RLM befassen müssen.

In Ausnahmefällen ist es jedoch notwendig, neue RLM-Software in das FlashROM Ihrer RLMs zu laden. Dies ist beispielsweise in den folgenden Situationen der Fall:

- Wenn Sie das RLM aktualisieren möchten, damit es neue Funktionen unterstützt.
- Wenn Ihnen dies vom technischen Support von Siemens empfohlen wurde.
- Wenn Sie einen erzwungenen Neustart ausführen müssen.

Die RLM-Software ist eine Binärdatei im Format "wpntxxx.bin", wobei "*xxx*" für die Version der RLM-Software steht.

Sie finden eine Kopie dieser Datei in dem Verzeichnis, in dem Sie die Anwendung RLM Manager installiert haben. Die neueste Version der Radio Link-Modul-Software finden Sie jeweils auf der Siemens **http://www.siemens.com/mobic**-Website.

D.2 Laden der Software

Beim Laden der RLM-Software (oder Firmware) werden keine Änderungen an der Konfiguration des RLM vorgenommen. Es empfiehlt sich jedoch, anhand der Option **Download Config File** im RLM-Menü eine Sicherungskopie zu erstellen, falls keine Sicherungsdatei der aktuellen Konfigurationseinstellungen existiert.

1. Wählen Sie das Ziel-RLM in der Liste aus, oder geben Sie eine IP - Adresse für ein bestimmtes Radio Link-Modul ein.
2. Wählen Sie die Option **Upload Software** im RLM-Menü.
   Die Anwendung RLM Manager fordert Sie zum Öffnen einer Access Point RLM-Softwaredatei (*.bin) auf.
3. Wechseln Sie zum Installationsverzeichnis der Anwendung RLM Manager, oder zu dem Verzeichnis, in dem die Access Point RLM-Softwaredatei gespeichert ist, die Sie von der Siemens SIMATIC NET IWL-Website heruntergeladen haben.
4. Wählen Sie in der Liste der angezeigten Dateien die Datei "wpntxxx.bin", wobei "xxx" für die Version der Access Point RLM-Software steht.
5. Klicken Sie auf die Schaltfläche **Öffnen**, um die RLM-Softwaredatei zu öffnen.
6. Geben Sie das Kennwort für das RLM ein, wenn Sie dazu aufgefordert werden, und klicken Sie auf **OK** , um den Vorgang fortzusetzen.
7. Wenn Sie zum Bestätigen des Ladens der RLM-Software aufgefordert werden, klicken Sie auf **Yes**.

   Das RLM wird neu gestartet und nimmt den Bridging-Betrieb auf. Dabei verwendet es die Parameter, die in der Softwaredatei festgelegt wurden.

D.2.1 Bestätigen des Ladevorgangs der RLM-Software

Wenn Sie die RLM-Softwaredatei (*.bin) auf das RLM laden möchten, werden Sie in einem Meldungsfenster zunächst zum Bestätigen der folgenden Vorgänge aufgefordert:

- Das Laden der Softwaredatei auf das RLM.
- Das Überschreiben der RLM-Softwaredatei (*.bin), die Sie für den Ladevorgang auf das RLM ausgewählt haben.

Bei diesem Vorgang wird die RLM-Softwaredatei zwar überschrieben, jedoch wirkt sich dies nicht auf ihre Funktionalität oder Eigenschaften aus.

D.2.1.1 Die Option "Yes, Upload RLM Software"

Wenn Sie die Option "Yes, Upload Access Point RLM Software" wählen, führt die Anwendung
RLM Manager Folgendes aus:

1. Sie speichert zunächst die Radio Link-Modul-Softwaredatei mit dem gleichen Dateinamen auf dem Datenträger, d.h., die geöffnete Softwaredatei wird überschrieben.
2. Anschließend lädt sie die gespeicherte Datei auf das Ziel-Radio Link-Modul.

Beim Speichern der RLM-Softwaredatei auf dem Datenträger wird der Abschnitt der Softwaredatei, der die Konfigurationsparameter enthält, mit den Einstellungen aktualisiert, die vom RLM abgerufen oder aus der Sicherungsdatei (*.cnf) importiert wurden. Der Abschnitt für Software der

RLM-Softwaredatei bleibt unverändert (weitere Informationen siehe Funktionsweise des Ladevorgangs (Seite 294).

Da der Abschnitt für Software unverändert bleibt, wirkt sich das Überschreiben der Softwaredatei nicht auf die Funktionalität oder die Eigenschaften dieser Datei aus.

D.2.1.2 Die Option "No, do not Upload RLM Software"

Wenn Sie die Option "No, do not Upload RLM Software" wählen, bricht die Anwendung RLM Manager den Ladevorgang ab.

Wenn Sie die RLM-Software trotzdem laden möchten, die ursprüngliche Softwaredatei jedoch nicht überschreiben wollen, sollten Sie eine Sicherungskopie dieser Datei (*.bin) erstellen und auf einem separaten Datenträger (Diskettenlaufwerk) speichern.

D.2.2 Funktionsweise des Ladevorgangs

Die RLM-Softwaredatei besteht eigentlich aus zwei Teilen, die im FlashROM des Access Point RLM gespeichert werden:

1. Der eigentlichen RLM-Firmware. Auf diese hat der Anwender keine Zugriffsmöglichkeit.
2. Den Konfigurationsparametern, die benutzerdefinierte Einstellungen für das Radio Link-Modul enthält. Die Daten in diesem Teil können jederzeit geändert werden, wenn Sie mit Hilfe der Anwendung RLM Manager eine Remote-Konfigurationsdatei öffnen und speichern.

Der Vorgang zum Laden der Software auf das Radio Link-Modul erfolgt, indem die Anwendung RLM Manager die vom RLM abgerufenen Konfigurationsparameter mit der Firmwaredatei (*.bin) zusammenführt. Diese werden zunächst auf dem Datenträger gespeichert, bevor sie auf das RLM geladen werden.

E Weitere Unterstützung

E.1 Ansprechpartner

Wenn Sie technische Fragen zum Einsatz des hier beschriebenen Produktes haben und das Problem mit Hilfe der Dokumentation oder des integrierten Hilfesystems nicht lösen können, wenden Sie sich an Ihren Ansprechpartner bei Siemens oder Ihren Siemens-Fachhändler.

Die Adressen finden Sie:

- in unserem Katalog IK PI oder CA01
- im Internet (http://www.siemens.com/simatic-net)

E.2 Automation and Drives, Service & Support

Service & Support von A&D ist weltweit rund um die Uhr erhältlich.

Die Service- und Supportleistungen können in deutscher und englischer Sprache erfolgen.
An der Autorisierungs-Hotline wird darüber hinaus Französisch, Italienisch und Spanisch gesprochen.

Abbildung 47 Service und Support



<table>
<tr><th>Technischer Support</th><th>Autorisierungs-Hotline</th></tr>
<tr><td>Europa und Afrika (Nürnberg)
Mo. bis Fr. 7:00 bis 17:00
Uhr (Ortszeit, GMT +1)Tel.: +49 - (0) 180 - 5050 - 222
Fax: +49 - (0) 180 - 5050 - 223
E-Mail: techsupport@ad.siemens.de</td><td>Europa und Afrika (Nürnberg)
Mo. bis Fr. 7:00 bis 17:00
Uhr (Ortszeit, GMT +1)Tel.: +49 - (0) 911 - 895 - 7200
Fax: +49 - (0) 911 - 895 - 7201
E-Mail: authorization@nbgm.siemens.de</td></tr>
<tr><td colspan="2" align="center">Amerika (Johnson City)
Mo. bis Fr. 8:00 bis 19:00
Uhr (Ortszeit, GMT -5)Tel.: +1 - (0) 423 - 262 - 2522
Fax: +1 - (0) 423 - 262 - 2231
E-Mail: simatic.hotline@sea.siemens.com</td></tr>
<tr><td colspan="2" align="center">Asien und Australien (Singapur)
Mo. bis Fr. 8:30 bis 17:30
Uhr (Ortszeit, GMT +8)Tel.: +65 - (0) 740 - 7000
Fax: +65 - (0) 740 - 7001
E-Mail: simatic.hotline@sae.siemens.com.sg</td></tr>
</table>

SIMATIC-Sonder-Hotline	
Weltweit (Nürnberg) Werktags 0:00 bis 24:00 Uhr (Ortszeit, GMT +1)Tel.: +49 - (0) 911 - 895 - 7777 Fax: +49 - (0) 911 - 895 - 7001 E-Mail: techsupport@ad.siemens.de	Schneller Rückruf innerhalb von maximal zwei Stunden garantiert (geführenpflichtig, nur mit SIMATIC-Karte)

E.3 Service & Support im Internet

Im World Wide Web finden Sie stets die neuesten Informationen zur gesamten SIMATIC-Produktreihe - beispielsweise häufig gestellte Fragen (Frequently Asked Questions, FAQs), Tipps und Tricks, Software-Aktualisierungen und Informationen für Benutzer.

Neben diesen kostenlosen Informationen können Sie gegen Gebühr auch Folgendes anfordern:

- Software-Produkte
- Beispiele für Anwendungsprogramme

Die Abrechnung erfolgt über die SIMATIC-Karte.

Internet-Adresse:

http://www.siemens.de/automation/service&support

Sie können auch eine Frage im SIMATIC Knowledge Manager stellen, der in der Wissensdatenbank nach entsprechenden Lösungen sucht.

Wenn Sie sich an einem Standort ohne Onlinezugang befinden, finden Sie einen Teil der kostenlos verfügbaren Informationen auf der "SIMATIC Customer Support Knowledge Base"-CD.

E.4 Training für SIMANTIC NET

Ansprechpartner für Trainingskurse:

Siemens AG
Trainings-Center für Automatisierungs- und Antriebstechnik
A&D PT 49 Kursbüro

Östliche Rheinbrückenstraße 50
76181 Karlsruhe
Deutschland

Tel.: +49 - (0) 721 - 595 - 2917

Fax: +49 - (0) 721 - 595 - 6087

Internet: http://www.sitrain.com

E.5 Zertifizierung

Die Produkte von SIMATIC NET werden nach einem Qualitätsmanagementsystem hergestellt und vermarktet, das DIN ISO 9001 entspricht und durch DQS zertifiziert ist (Zertifikat-Registriernummer. 2613). Das DQS-Zertifikat wird in allen IQNet-Ländern anerkannt (Registriernummer: 2613).

Glossar

A

Acess Control

Eine Sicherheitsfunktion des Radio Link-Moduls, mit der Sie den drahtlosen Zugriff auf einen Access Point auf berechtigte Stationen beschränken können.

Berechtigte Stationen sind durch die MAC-Adresse ihrer SIMATIC NET IWL PC Card in einer so genannten Zugriffskontrolltabellendatei gekennzeichnet, die als Teil der Konfiguration auf die SIMATIC NET IWL-Access Points geladen wird.

Bei aktivierter Zugriffskontrolle ignoriert das Radio Link-Modul alle Anforderungen zum Weiterleiten von Daten von/an SIMATIC NET IWL-Geräte, die nicht in der Zugriffskontrolltabelle eingetragen sind. Sie können Zugriffskontrolltabellendateien mit Hilfe des RLM Managers oder der Anwendung CP 1515 erstellen oder bearbeiten.

Acess Control Table

Eine ASCII-Tabelle mit sämtlichen MAC-Adressen der Stationen, die zum Senden/Empfangen von Daten über das Radio Link-Modul

berechtigt sind. Sie können Zugriffskontrolltabellen mit Hilfe der Anwendung RLM Manager erstellen.

Die Access Control Table wird im Rahmen der Aktualisierung der Konfiguration des Radio Link-Moduls geladen.

Analysis Polling Interval

Ein Parameter, mit dessen Hilfe Sie die Ansprechempfindlichkeit des Remote-Link-Tests im SIMATIC NET IWL RLM Manager steuern können. Das Analyse-Abfrageintervall bestimmt, wie oft der RLM Manager die Diagnoseparameter der Bridge-Einheit abliest. Gültige Werte: 1-15 Sekunden.

Siehe auch: Überwachen des SIMATIC NET IWL-Netzes (page 73)

B

Basic Access-Netzwerk

Ein Basic Access-Netzwerk ist ein klein dimensioniertes LAN ohne Verbindungen über Gateways oder Router. Die Anzahl der Radio Link-Module in diesem Netzwerk schwankt in der Regel zwischen 1 und 5. Auf den Administrator-Stationen muss der TCP/IP-Protokollstapel geladen sein. Außerdem muss die Konfiguration und Überwachung der RLMs über IP-Adressen erfolgen. Für die Client-Stationen ist die IP-Adressierung und das TCP/IP-Protokoll nicht unbedingt erforderlich.

Betriebszeit

Die seit dem letzten Einschalten, Zurücksetzen oder Aktualisieren des RLM-Geräts mit einer neuen Konfiguration verstrichene Zeit.

BOOTP (Bootstrap-Protokoll)

Das zum Konfigurieren von netzwerkübergreifenden Systemen verwendete Standardprotokoll.

BootROM

Ein Speicherchip im Access Point RLM, der die Startkonfiguration des Access Points enthält. Wenn Sie die Konfiguration eines RLM-Geräts ändern, werden die Werte der Konfigurationsparameter im BootROM gespeichert.

Bridge in

Die Summe der Datenpakete, die das RLM vom LAN-Segment über die gewählte drahtlose Netzwerkschnittstelle empfängt.

Dieser Wert gibt die Summe der Unicast- und Nicht-Unicast-Pakete wieder.

Siehe auch: RLM Manager, Überwachen, Remote-Statistik

Bridge in discards

Die Summe der nicht vom RLM akzeptierten Datenpakete.

Siehe auch: RLM Manager, Überwachen, Remote-Statistik

Bridge out

Die Summe der Datenpakete, die vom RLM über die gewählte drahtlose Netzwerkschnittstelle an das LAN-Segment weitergeleitet wurden.

Siehe auch: RLM Manager, Überwachen, Remote-Statistik

Bridge Priority

Ein Bridge-Konfigurationsparameter, mit dessen Hilfe Sie die Auswahl der 'Root Bridge' und der 'Designated Bridge' beeinflussen können, die vom Spanning Tree-Algorithmus berechnet werden. Besitzt der Parameter 'Bridge Priority' einen niedrigen Wert, besteht eine größere Wahrscheinlichkeit, dass die Bridge als 'Designated Bridge' oder 'Root Bridge' ausgewählt wird (in der Regel '0'). Der empfohlene Wert ist '32768'. Gültige Werte: 0-65000, Anfangswert: '32768'.

Siehe auch: RLM Manager, Bridge-Konfigurationsparameter

Broadcast

Von einer Station (in der Regel ein Server) an alle Stationen im Netzwerk übertragene Meldungen. Diese Art des Netzverkehrs bezeichnet man auch als Nicht-Unicast-Meldungen.

Bytes in

Die Summe Byte (Oktette), die das RLM vom LAN-Segment über die gewählte drahtlose Netzwerkschnittstelle, einschließlich Rahmencharakteristika, empfängt.

Siehe auch: RLM Manager, Überwachen, Remote-Statistik

Bytes out

Die Anzahl der von Protokollen einer höheren Ebene angeforderten Frames, die an eine Nicht-Unicast-Adresse (d.h. eine Subnetz-Broadcast- oder Subnetz-Multicast-Adresse) übertragen werden sollen. Diese Zahl schließt die verworfenen oder nicht gesendeten Frames ein.

Siehe auch: RLM Manager, Überwachen, Remote-Statistik

D

DHCP (Dynamic Host Configuration Protocol)

DHCP ist eine proprietäre Erweiterung des vorhandenen Bootstrap-Protokolls (BOOTP) von Microsoft. Mit Hilfe von DHCP kann der LAN-Administrator die Arbeitsstationen dynamisch und ohne weiteres Eingreifen über den Netzwerkserver mit IP-Adressen konfigurieren.

Eine dynamisch zugewiesene IP-Adresse wird auch als "Aktivlease" bezeichnet. Aktivleases besitzen in der Regel ein Ablaufdatum. Hierdurch wird die Neuzuweisung von IP-Adressen ermöglicht, die nicht mehr verwendet werden.

Es empfiehlt sich, für Radio Link-Module eine spezielle IP-Adresse zu verwenden, für die kein Ablaufdatum festgelegt ist. Verwenden Sie Ihr DHCP-Verwaltungsprogramm zum Reservieren der IP-Adresse oder eines Bereichs von IP-Adressen.

Für Netzwerkgeräte, die eine bestimmte IP-Adresse erfordern, oder für die die "IP-Adresslease" nicht ablaufen soll, können Sie mit Hilfe eines DHCP-Verwaltungsprogramms eine IP-Adresse reservieren. Dies ist bei Radio Link-Modulen der Fall.

Nachdem ein Bereich von IP-Adressen reserviert wurde, können Sie Ihrem SIMATIC NET IWL-System die Werte in diesem Bereich zuweisen.

Die eindeutige Kennung ist die MAC-Adresse (Media Access Control, MAC) des DHCP-Clients. Als Clientname sollte der Computername des DHCP-Clients verwendet werden. Dieser Name wird nur zu Identifikationszwecken in der DHCP-Verwaltungsschnittstelle verwendet und muss daher nicht mit dem tatsächlichen Computernamen übereinstimmen bzw. wirkt sich nicht auf diesen aus.

Um festzustellen, welche IP-Adressen noch verfügbar sind, beinhalten die DHCP-Verwaltungsprogramme in der Regel eine Option zum Ermitteln der aktiven Leases. Anhand dieser Option können Sie feststellen, welchen DHCP-Clients eine IP-Adresse vom DHCP-Server zugewiesen wurde.

F

Filter-Alterungszeit

Radio Link-Module führen dynamische Listen zum Kennzeichnen der Schnittstelle, bei der sie zuletzt eine SIMATIC NET IWL-Station

(entweder die Ethernet-Schnittstelle oder die SIMATIC NET IWL-Schnittstelle A oder B) gefunden haben.

Wenn das RLM ein Paket empfängt, das an eine bestimmte Station adressiert ist, kann das RLM anhand dieser Liste feststellen, über welche Schnittstelle das Paket transferiert werden soll.

Wenn mobile Stationen sich bei verschiedenen Netzwerkzellen anmelden (Roaming), wird diese Tabelle automatisch aktualisiert.

Wenn über einen längeren Zeitraum kein Verkehr von oder zu einer bestimmten Station erfolgt (z.B. wenn die Station heruntergefahren wurde), bestimmt die Filter-Alterungszeit, wie lange der Access Point sich an den Standort dieses SIMATIC NET IWL-Geräts "erinnert".

Firmware

Die werksseitig vorinstallierte Betriebssoftware für die SIMATIC NET IWL PC Card und das Radio Link-Modul.

Wenn neue Funktionen für das SIMATIC NET IWL-Produkt entwickelt wurden, werden diese möglicherweise in Form von Firmware-Updates zur Verfügung gestellt.

Firmware-Update

Dabei handelt es sich um ein Update für die Software, die auf Ihrem SIMATIC NET IWL-Produkt installiert ist.

- Für die SIMATIC NET IWL PC Card werden Firmware-Updates als ausführbare Datei im Format "wsuVVxxx.exe" bereitgestellt, wobei "xxx" für die Version des Updates steht. Diese ausführbare

Datei wird ein Mal auf dem Computer mit der PC Card ausgeführt.

- Für Access Point RLMs werden Firmware-Updates als Binärdatei im Format "wpntxxx.bin" bereitgestellt, wobei "xxx" für die Version der Firmware steht. Aktualisieren Sie die Firmware des Radio Link-Moduls anhand der Option **Upload Software** im Menü "Access Point" der Anwendung RLM Manager.

H

Hello Time

Ein Spanning Tree-Parameter, der das Zeitintervall zwischen der Übertragung von Konfigurations-BPDU-Meldungen über eine Root Bridge oder über eine Bridge angibt, die zur Root Bridge werden will.

Empfohlener Wert: 2 Sekunden.

I

Initiator-Station

Das (entfernte) Access Point RLM-Gerät, das einen Remote Link-Test auf einer drahtlosen Station einleiten soll, die mit dem ausgewählten Radio Link-Modul verbunden ist.

Der Remote Link-Testpartner kann entweder eine drahtlose Station oder ein weiteres RLM-Gerät sein.

IP-Adresse

Die IP-Adresse (Internet Protocol, IP) ist ein eindeutiger Adresscode für Datenverarbeitungsgeräte. Wenn in Ihrem Netzwerk bereits die IP-Adressierung verwendet wird, müssen Sie die werksseitig eingestellte IP-Adresse auf einen Wert im Bereich der IP-Adressen einstellen, der Ihrem Unternehmen zugewiesen ist.

K

Kernel

Siehe 'Firmware'

Kollisionen

Die Anzahl der Pakete, die aufgrund von Kollisionen nicht ordnungsgemäß empfangen wurden, wenn mehrere Stationen gleichzeitig versucht haben, Pakete über das Medium zu senden.

Siehe auch: RLM Manager, Überwachen, Remote-Statistik

L

LAN-Segment

Ein logischer Bereich in einem Netzwerk, der über eine Bridge mit anderen Netzwerkbereichen verbunden ist.

Im Falle von Radio Link-Modulen können diese Bereiche entweder Ethernet- oder SIMATIC NET IWL-Segmente sein. Im Falle von Access Points (RLMs) können sogar zwei SIMATIC NET IWL-Segmente existieren (A und B). Jedes SIMATIC NET IWL-Segment ist durch eine eindeutige Netzwerkkennung gekennzeichnet.

Link-Test

Eine SIMATIC NET IWL-Diagnoseoption, mit der Sie eine bestimmte Verbindung zwischen zwei drahtlosen Stationen überprüfen können.

Anhand des Link-Tests können Sie die Qualität der drahtlosen Kommunikation analysieren und die Platzierung von Stationen und Antennen bestimmen oder optimieren.

M

MAC-Adresse

Eine Hexadezimalzahl mit 16 Ziffern, die ein Netzwerkgerät im Netzwerk kennzeichnet.

MAC-Adressfilter

Ein erweiterter Bridge-Konfigurationsparameter für Radio Link-Module, mit dessen Hilfe Sie den Datenverkehr zwischen zwei bestimmten Geräten über die drahtlose(n) Schnittstellen(n) der Access Point-Bridge beschränken können.

Anhand des statischen MAC-Adressfilters können Sie die Leistungsfähigkeit eines drahtlosen (sowie eines verkabelten) Netzwerks optimieren.

Um beispielsweise zu verhindern, dass redundanter Verkehr über das drahtlose Netzwerk übertragen wird, können Sie den Verkehr zwischen zwei bestimmten Servern, die durch ihre MAC-Adresse und den vom Access Point RLM (am drahtlosen oder verkabelten Bridge-Port) ermittelten Standort gekennzeichnet sind, einschränken.

In den meisten Fällen ist es jedoch einfacher, redundanten Verkehr über andere Filteroptionen, wie beispielsweise die Protokollfilterung, zu kontrollieren.

Max Age

Ein erweiterter Bridge-Konfigurationsparameter für Radio Link-Module, mit dessen Hilfe Sie den Datenverkehr durch den Access Point RLM bestimmen können.

Wenn die Bridge Protokollinformationen empfängt, die den Wert ’Max. Age’ überschreiten, verwirft die Bridge diese Informationen und startet den Zeitgeber für die Weiterleitungsverzögerung, damit andere Bridges die aktualisierten Topologieinformationen weiterleiten können (z.B., wenn eine andere Bridge zur "Root Bridge" geworden ist).

Empfohlener Wert: 20 Sekunden.

Multicast

Von einer Station (in der Regel ein Server) an mehrere Stationen im Netzwerk übertragene Meldungen. Diese Art des Netzverkehrs bezeichnet man auch als Nicht-Unicast-Meldungen.

Multicast-Mechanismus

In Netzwerkumgebungen mit mehreren RLMs verhindert der Multicast-Mechanismus Framekollisionen, wenn mehrere Access Points gleichzeitig versuchen, auf das drahtlose Medium zuzugreifen, beispielsweise bei Meldungen, die von einer Station an mehrere Stationen (Multicast) oder alle Stationen (Broadcast) im Netzwerk übertragen werden.

Der standardmäßige Multicast-Mechanismus generiert eine zufällige Verzögerung für jede drahtlose Schnittstelle eines Radio Link-Moduls. Die zufällige Verzögerung basiert auf den letzten Ziffern der MAC-Adresse der installierten SIMATIC NET IWL PC Card.

Optional können Sie eine 'benutzerdefinierte' Multicast-Verzögerung im Bereich von 1-10 definieren.

Siehe auch: RLM Manager Bearbeitungsparameter

N

Non-Unicast packets in

Die Anzahl der an ein höheres Protokoll übertragenen Nicht-Unicast-Pakete, in der Regel Multicast- oder Broadcast-Meldungen.

Siehe auch: RLM Manager Remote-Statistik

Non-Unicast packets out

Die Anzahl der von höheren Protokollen angeforderten Pakete, die an eine Subnetz-Unicast-Adresse übertragen werden sollen, in der Regel Multicast- oder Broadcast-Meldungen. Diese Zahl schließt die verworfenen oder nicht gesendeten Frames ein.

Siehe auch: RLM Manager Remote-Statistik

O

Option "Read Password"

Eine Sicherheitsoption, die es Ihnen erlaubt, mit Hilfe eines Kennworts eine Netzwerkverwaltungsebene zu erstellen.

Das Kennwort für Lesevorgänge in Verbindung mit der richtigen IP-Adresse erlaubt einem lokalen LAN-Administrator nur das Anzeigen der Monitor-Funktion von RLM Manager, jedoch nicht das Anzeigen oder Ändern der Access Point-Konfiguration.

Sie können das Kennwort für Lesevorgänge auf der Registerkarte "SNMP" in der Anwendung RLM Manager festlegen.

Option "Read/Write Password"

Eine Sicherheitsoption, die es Ihnen erlaubt, mit Hilfe eines Kennworts eine Netzwerkverwaltungsebene zu erstellen.

Das Kennwort für Lese-/Schreibvorgänge in Verbindung mit der richtigen IP-Adresse erlaubt es einem Unternehmens-LAN-Administrator, alle Monitor-Funktionen von RLM Manager anzuzeigen sowie die Konfiguration des Radio Link-Moduls anzuzeigen und zu bearbeiten.

Sie können das Kennwort für Lese-/Schreibvorgänge auf der Registerkarte "SNMP" in der Anwendung RLM Manager festlegen.

Out Collisions

Die Anzahl der erfolgreich von einer bestimmten Schnittstelle übertragenen Frames, für die die Übertragung durch genau eine oder mehrere Kollisionen plus die Zahl der auf einer bestimmten Schnittstelle nach 512-Bit-Takten seit Beginn der Übertragung eines Pakets festgestellten Kollisionen verhindert wurde.

Siehe auch: RLM Manager Remote-Statistik

P

Packets received/lost

Der ’Packets received/lost’-Zähler zeigt den Prozentsatz der empfangenen Pakete im Verhältnis zur Anzahl der erwarteten Pakete an. Der ’Packets received/lost’-Zähler wird nur angezeigt, wenn Sie die Option "View Details" auswählen.

Siehe auch: CP 1515-Link-Test

Path cost

Ein erweiterter Bridge-Konfigurationsparameter für Radio Link-Module, der zum Bestimmen der bevorzugten Datenpfade zwischen den Bridges im Netzwerk und der ’Root Bridge’ verwendet wird, die vom ’Spanning Tree-Algorithmus’ berechnet wird.

Die ’Root-Bridge’ überträgt BPDU-Telegramme an das gesamte LAN. Wenn eine Bridge eine BPDU-Telegramms an einem ihrer Ports empfängt, addiert sie den Wert im Feld "Path Cost" für diesen Port vor dem Weiterleiten der Meldung zum Wert im Feld "Root path cost" der BPDU-Meldung. Hiermit können die anderen Bridges den Wert des Parameters ’Total Path Cost’ für die Übertragung zur Root Bridge über diesen Port bestimmen.

Ein niedrigerer ’Path Cost’-Wert würde in der Regel für Ports zu LAN-Segmenten verwendet, die näher bei der Root Bridge liegen. Ein höherer ’Path Cost’-Wert würde in der Regel für Ports zu LAN-Segmenten verwendet, die "Knoten" der Spanning Tree-Struktur sind.

Wenn Sie das Access Point RLM beispielsweise als Access Point für drahtlose Stationen zum Ethernet verwenden, würde ein hoher Wert des Parameters 'Path Cost' für den SIMATIC NET IWL-Port die unnötige Nutzung der Bandbreite des drahtlosen Mediums minimieren (empfohlener Wert 500).

Peer-to-Peer-Arbeitsgruppe

Eine eigenständige Arbeitsgruppe drahtloser Stationen, die Mitglieder eines kleinen (Peer-to-Peer) Netzwerks sind. Dies ist in der Regel eine SIMATIC NET IWL-Netzwerkkonfiguration ohne RLMs, die die Stationen mit der Netzwerkinfrastruktur verbinden würden.

Diese Stationen müssen für den Betrieb im Peer-to-Peer-Modus konfiguriert werden.

Port Priority

Ein erweiterter Bridge-Konfigurationsparameter für das Access Point RLM, mit dessen Hilfe Sie beeinflussen können, welcher Port in den Spanning Tree einbezogen werden soll, wenn mehrere Bridge-Ports einer einzelnen Bridge-Einheit in einer Schleife verbunden sind.

Ein niedrigerer Wert erhöht die Wahrscheinlichkeit, dass ein Port im Spanning Tree ausgewählt wird, wenn ein anderer Port einen höheren Wert aufweist. Gültige Werte: 0-255. Anfangswert: '128'

R

Rauschpegel

Der Rauschpegel gibt den Pegel des lokalen Hintergrundrauschens an, der an der drahtlosen Schnittstelle des Access Point RLM gemessen wurde. Der Rauschpegelzähler gibt nur den Rauschpegelwert (in %) des letzten Frames wieder, das an der Schnittstelle empfangen wurde.

Siehe auch: CP 1515-Link-Test

Remote Link-Test

Eine SIMATIC NET IWL-Diagnoseoption der Anwendung CP 1515. Anhand des Remote Link-Tests können Sie die Verbindungsqualität zwischen einem Remote-RLM und einer Station analysieren, die mit der ausgewählten RLM-Einheit verbunden ist.

Diese Option wird oftmals zum Überprüfen von drahtlosen Außenverbindungen oder zum Analysieren der Verbindungsqualität von drahtlosen Stationen in einem Remote-Netzwerk verwendet.

Roaming

Dabei handelt es sich um eine Funktion, die es mobilen SIMATIC NET IWL-Geräten erlaubt, sich an verschiedenen physikalischen Standorten in der LAN-Umgebung anzumelden.

Um das Roaming zu ermöglichen, müssen diese Standort von einem Access Point RLM bedient werden.

Die Roaming-Funktionalität überwacht die Qualität der Kommunikation über die RLMs und stellt gegebenenfalls automatisch eine Verbindung zu einem anderen Access Point her, um die Netzwerkverbindung aufrecht zu erhalten.

Das Roaming ist nur innerhalb einer Domäne möglich, d.h., solange sich die mobile Station in Reichweite der Radio Link-Module befindet, die den gleichen drahtlosen Netzwerknamen besitzen.

S

Signal

Eine Meldung, die in regelmäßigen Abständen vom RLM an alle drahtlosen Stationen in der Domäne übertragen wird. Anhand von SignalMeldungen wird die Kommunikation verwaltet und optimiert, indem die mobilen SIMATIC NET IWL-Stationen beim Herstellen einer automatischen Verbindung zum Access Point unterstützt werden, der die beste Kommunikationsqualität bietet.

Signalpegel

Der Signalpegel gibt die Stärke des SIMATIC NET IWL-Signals an, das an der drahtlosen Netzwerkschnittstelle empfangen wird.

Site Monitor

Eine SIMATIC NET IWL-Diagnoseoption der Anwendung CP 1515, mit deren Hilfe Sie die Kommunikationsqualität verschiedener Access

Point RLMs gleichzeitig anzeigen können. Sie können anhand von Site Monitor die Flächenabdeckung Ihres SIMATIC NET IWL-Netzwerks untersuchen und Site-Überprüfungen vornehmen.

Site-Überprüfung

Ein Verfahren zur Bestimmung oder Optimierung der Platzierung Ihrer Radio Link-Module.

Siehe auch: Site Monitor.

SNMP (Simple Network Management Protocol)

Ein Standard-Netzwerkprotokoll für die lokale oder weltweite Verwaltung von Netzwerken über das Internet.

SNMP-IP-Zugriffsliste

Eine erweiterte Sicherheitsoption, mit deren Hilfe Sie eine beschränkte Gruppe von SNMP-Verwaltungsstationen zur SNMP-Verwaltung berechtigen können.

Wenn Sie eine Station für den Zugriff auf die RLM-Konfigurations- oder -Diagnoseinformationen berechtigen wollen, müssen Sie die IP-Adresse dieser Station zur so genannten SNMP-IP-Zugriffsliste hinzufügen.

Bei Aktivierung der SNMP-IP-Zugriffsoption lehnt das RLM alle Anforderungen zum Lesen der Konfigurationsdaten oder Diagnosezähler ab, wenn die IP-Adresse der anfordernden Station nicht in der SNMP-IP-Zugriffsliste registriert ist.

Sie können die SNMP-IP-Zugriffsliste in Verbindung mit anderen Sicherheitsoptionen wie den Kennwörtern für Lesevorgänge bzw. für Lese-/Schreibvorgänge verwenden.

Die SNMP-IP-Zugriffsliste können Sie über die Registerkarte "SNMP" der Anwendung RLM Manager erstellen oder bearbeiten.

SNMP-Abfrageintervall

Ein Parameter, mit dessen Hilfe Sie die Ansprechempfindlichkeit der Monitor-Optionen von RLM Manager steuern können. Gültige Werte: 1 Sekunde - 5 Minuten.

SNMP-Trap-Nachrichten

SNMP-Trap-Nachrichten sind Bestandteil des Trap Host-Mechanismus, der den Netzwerkadministrator darüber informiert, wenn ein Access Point RLM zurückgesetzt, eine neue Konfiguration auf den Access Point geladen oder ein erzwungener Neustart ausgeführt wird.

Die Trap Host-Nachricht erlaubt es dem Netzwerkadministrator, festzustellen, ob die jeweilige Aktion berechtigt war.

Damit die Verwaltungsstation Trap-Nachrichten empfangen kann, muss ein Trap Empfänger für die Verarbeitung der Trap-Nachrichten installiert sein.

Spanning Tree

Eine erweiterte Bridge-Konfigurationsoption für komplexe Netzwerktopologien, anhand der Sie die Effizienz des Netzverkehrs optimieren und eventuelle Datenschleifen vermeiden können.

Mit Hilfe des Spanning Tree-Algorithmus tauschen die Bridges im LAN spezielle Konfigurationsnachrichten untereinander aus, die ihnen Folgendes erlauben:

- Die Wahl einer Bridge zur ’Root Bridge’. Die Auswahl erfolgt aus sämtlichen Bridges in den verbundenen LAN-Segmenten.
- Die Berechnung des kürzesten Pfades zur ’Root Bridge’.
- Die Wahl einer ’Designated Bridge’ in jedem LAN-Segment, die Pakete von diesem LAN-Segment an die ’Root Bridge’ weiterleitet.

Die Wahl eines ’Root Ports’ aus den Ports der Bridge-Einheit.

Der Spanning Tree-Algorithmus erlaubt es den Bridges, ein schleifenloses Subnetz der LAN-Topologie (eine Baumstruktur) zu berechnen, das die höchstmögliche Konnektivität zwischen zwei physikalisch verbundenen LAN-Segmenten bietet.

Wenn ein Fehler auf dem kürzesten Datenpfad auftritt (beispielsweise aufgrund eines physikalischen Ausfalls), erstellt der Spanning Tree-Algorithmus die Topologie innerhalb der Beschränkungen der verfügbaren überbrückten LAN-Komponenten neu.

SRV (Signal-/Rauschverhältnis)

Das Signal-/Rauschverhältnis (SRV) ist der primäre Diagnosezähler zur Überprüfung der Leistungsfähigkeit der drahtlosen Geräte. Das SRV gibt die relative Stärke des empfangenen Signalpegels im Verhältnis zum lokalen Rauschpegel an.

Stationsadresse

Die Stationsadresse ist eine eindeutige Kennung, die auf jeder SIMATIC NET IWL PC Card und jedem Radio Link-Modul gespeichert wird. Das für die Stationsadressen verwendete Adress-System entspricht den Richtlinien für universelle MAC-Adressen. Die Stationsadresse ist ein alphanumerischer Code aus 12 Ziffern, der sich aus zwei Blöcken zu je 6 Hexadezimalzahlen zusammensetzt (siehe auch "“MAC-Adresse”").

Stationsname

Der Stationsname ist ein optionaler Parameter zur Kennzeichnung drahtloser Geräte im Netzwerk. Der Name kann auch das Finden eines Geräts in einem der SIMATIC NET IWL-Diagnoseprogramme erleichtern. Ein Stationsname kann aus maximal 31 alphanumerischen Zeichen bestehen.

Storm Threshold

Eine erweiterte Bridge-Konfigurationsoption, mit der Sie das Netzwerk vor Datenüberlastung schützen können, indem Sie Folgendes festlegen:

- Die maximale Anzahl Frames pro Sekunde, die von einem Netzwerkgerät (gekennzeichnet durch seine MAC-Adresse) empfangen werden können.
- Das absolute Maximum der Meldungen pro Port.

Die 'Storm Threshold'-Parameter erlauben es Ihnen, eine Reihe von Schwellenwerten für die einzelnen Ports des Radio Link-Moduls festzulegen, wobei Sie separate Werte für die Anzahl der Broadcast-Meldungen pro Sekunde und der Multicast-Meldungen pro Sekunde angeben können.

Wenn die Anzahl der Frames für einen Port oder eine Station den Maximalwert pro Sekunde überschreitet, ignoriert der Access Point alle nachfolgenden Meldungen von diesem Netzwerkgerät oder alle Meldungen dieses Typs.

Subnetz

Ein Subnetz ist ein logischer Teilbereich eines LANs, das mit Hilfe von Routern oder Gateways in mehrere Bereiche aufgeteilt ist. Ein Subnetz kann mehrere LAN-Segmente umfassen.

Jedes Subnetz ist durch seine Subnetzmaske gekennzeichnet.

Hinweis: Das SIMATIC NET IWL-Roaming kann nicht über Router ausgeführt werden. Damit sich mobile Stationen bei verschiedenen drahtlosen Zellen anmelden können, müssen alle drahtlosen Stationen und Access Points mit dem gleichen LAN-Subnetz verbunden sein.

T

TTL (Time-To-Live)

Ein erweiterter IP-Parameter-Konfigurationszähler, den Sie zur Überwachung der Netzwerkeffektivität verwenden können. Der TTL-Zähler verhindert die endlose Weiterleitung von Nachrichtenframes mit falscher Adresse, die das Netzwerkmedium überlasten können.

Der TTL-Wert definiert die maximale Anzahl der Weiterleitungen pro Hop. Bei jeder Weiterleitung des Frames über einen Router verringert sich der TTL-Zähler um eins. Wenn der TTL-Zähler = 0 ist, wird das Frame abgewiesen.

U

Unicast packets in

Die Anzahl der Subnetzframes, die an ein höheres Protokoll übergeben werden. Dabei handelt es sich um die ’echten Daten’, die von Station zu Station weitergeleitet werden.

Unicast packets out

Die Anzahl Byte (Oktette), die an die Schnittstelle übertragen wurden.

Dabei handelt es sich um die ’echten Daten’, die von Station zu Station weitergeleitet werden.

Unternehmensnetzwerk

Eine Netzwerkkonfiguration, die als Unternehmens-LAN dimensioniert ist. Dieser Netzwerktyp kann Netzwerksegmente in verschiedenen Abteilungen umfassen, die über Bridges und Router miteinander verbunden sind. Wenn das Netzwerk auch Gateways, Router oder Bridges enthält, muss jedes Netzwerkgerät mit einer eindeutigen IP-Adresse gekennzeichnet werden. In das Netzwerk sind eventuell auch drahtlose Netzwerke in verschiedenen Gebäuden integriert, die miteinander über eine herkömmliche Verbindung, z.B. eine Mietleitung, verbunden sind.

V

Verschlüsselung

Eine Sicherheitsfunktion für Access Point RLMs und SIMATIC NET IWL-Stationen, die es Ihnen erlaubt, über das drahtlose Medium übertragene Daten zu verschlüsseln.

SIMATIC NET IWL-Produkte stehen optional auch mit einem werksseitig integrierten Verschlüsselungschip zur Verfügung, der auf dem WEP-Verschlüsselungsalgorithmus basiert.

Wenn Sie die Verschlüsselung in Ihrem drahtlosen Netzwerk verwenden möchten, muss auf allen SIMATIC NET IWL-Stationen und Access Points die Verschlüsselungsfunktion installiert und auf ’Enable’ (Aktiviert) gesetzt werden. Alle in der Netzwerkumgebung verwendeten Radio Link-Module und SIMATIC NET IWL-Geräte müssen den gleichen Chiffrierschlüssel benutzen.

Der Chiffrierschlüssel besteht aus 16 Hexadezimalzahlen im Bereich 0-9, A-F. Die zweite Ziffer jedes Ziffernpaars muss gerade sein (0,2,4,6,8,A,C,E).

W

Weiterleitungsverzögerung

Ein Zeitgeber für den Spanning Tree-Algorithmus, der verhindert, dass eine Bridge Datenpakete weiterleitet, wenn:

- die Bridge die Information empfängt, dass die aktive Spanning Tree-Topologie aktualisiert werden muss (z.B. wenn eine Bridge ausfällt oder wenn der Wert für die Parameter 'Bridge Priority' oder 'Path Cost' einer bestimmten Bridge geändert wurde);
- die Bridge feststellt, dass die Protokollinformationen den angegebenen Wert für 'Max. Age' überschreiten.

Änderungen in der Spanning Tree-Topologie müssen allen Bridges in einem überbrückten Netzwerk mitgeteilt werden. Der Zeitgeber für die Weiterleitungsverzögerung kompensiert die Übertragungsverzögerungen, die beim Weiterleiten der Protokollinformationen auftreten. Er erlaubt es den Bridges, alte Datenpfade zu schließen, bevor neue Datenpfade aktiviert werden.

Empfohlener Wert: 15 Sekunden

Windows-Arbeitsgruppe

Eine Windows-Arbeitsgruppe kann entweder aus drahtlosen oder aus verkabelten Netzwerkverbindungen oder einer Kombination dieser Verbindungsmöglichkeiten bestehen. In der Regel umfasst eine Windows-Arbeitsgruppe miteinander in Beziehung stehende

Mitglieder mit gemeinsamen Funktionen (z.B. Mitglieder einer Abteilung). Es ist für eine Windows-Arbeitsgruppe nicht von Bedeutung, wo sich die Mitglieder dieser Arbeitsgruppe befinden, da Mitglieder von Windows-Arbeitsgruppen durch ihren Arbeitsgruppennamen gekennzeichnet sind.

Stichwortverzeichnis

A

B

C

L

M

R

S

T

U